

May 2011
Issue 14

Magazine

NetworkSet

First Arabic Magazine for Networks

Data Link Flow Control Protocols

Cryptography Part II

wireless history

call hunting

الكتابلات

www.NetworkSet.net

NetworkSet

حرب العلم والمعرفة

المؤسس ورئيس التحرير
م. أيمن النعيمي

المحررون

السوريون

م. أنس الأحمد

م. رضوان سخيطة

المصريون

م. عادل الحميدي

م. نادر المنسي

م. مصطفى حسن

م. شريف مجدي

م. أحمد الشحات

العراقيون

م. محمد التميمي

ومفيدا لما قلت هذه الكلمة أبدا لأن الوصول إلى هذه الحقيقة بالنسبة لي أن هناك شخص من المئة شخص ولد الآن وهو أنت ولتان ردك لي أبشريا أخي فلقد أصبح الرقم اثنتان لأن النهضة العلمية بحسب وجهة نظري المتواضعة لن تقوم إلا بأيدي شباب وبنات يدركون هذه الحقيقة ويدركون أن المال والحكومات العربية التي فشلت في كل شيء ليست هي العائق الذي يقف أمامهم ويقف أمام مشروع النهضة العربية العلمية فهي الحرب الحقيقية التي يجب أن نخوض بها.

وسوف أقف معكم على حقيقة ما شاهدته من خلال الويكي الذي يثبت لي كل يوم أن أغلبكم لا يرى أبعد من أنفه فكيف له أن يرى خارج صندوقه فالدعوات التي وجهتها كثيرة والتسهيلات التي قدمتها أكثر ولكن أين أنتم ومن أنتم ؟

الكل يجلس ويقرأ ويستفيد من مايكته منتجي العالم العربي والذي أقدر عددهم بأحسن الأحوال بواحد بالمئة والتسعة وتسعين شخص يقول وأنا مالي في ستين داهية على قولة أخواننا المصريين. خلاصة هذا الكلام وأتمنى أن يأتي يوم وأخاطب كل من يقرأ هذا المقال بشكل شخصي حتى أقول له بصوت عالي أستيقظ وكفى بالله عليك نحن لا نتقدم أبدا للامام بل كل يوم في تراجع وقريبا جدا سوف يأتي اليوم الذي لن نستطيع مواكبة العالم والعلم لأن ما جعلنا نقف الآن في العالم هي مالدينا من موارد وهي في الآخر يجب أن تنتهي وعندها قنبلة نووية قد تكون خسارة فينا لكي يزيلوا هذه العاهة عن العالم وأعدروني لو أنني أنقلت عليكم في هذا المقال فأنا فعلا أتألم من هذا الوضع ولا أجد إلا هذه الكلمات لأعبر فيه عما يجول في نفسي لذا لنبدأ من اليوم وبهمة عالية تهز الجبال وبصوت واحد يقول فلتقرع الطبول فالحرب اليوم قد بدأت ودمتم بود.

مات بن لادن وأنتهت الحرب التي اخترعتها أمريكا والعالم الغربي على العرب والمسلمين ولكن من أنتصر في النهاية هل هو بن لادن أم أمريكا ؟ قد تكون حرب بن لادن التي شنها على الغرب خلفت مئة ألف قتيل أو مليون قتيل ولنقل عشرين مليون قتيل لكن هل أنتصر في النهاية ؟ جوابي هو أكيد لا فأمريكا والغرب من أنتصر في الحرب وحتى لو قتل بن لادن مئة مليون شخص سوف يبقى هم المنتصرين كون زمام العلم والتحكم مازالت في أيديهم وبقينا نحن على مكاننا في ملحق القائمة وليس في أسفلها ومازلنا نحتاج الكثير من الأشواط حتى نتأهل إلى قائمة دول العالم المتحضرة ومقالي أكيد لن يكون عن بن لادن وحروبه ضد الغرب فهو بالنسبة لنا كمسلمين ميت والميت لا تجوز عليه إلا الرحمة.

المعركة الحقيقة بالنسبة لي هي معركة العلم والمعرفة فهي من يرفع الشعوب والأمم وهي من ينزلها وليس المال كما يتصور البعض فالمال وسيلة تساعدنا على بناء الأمة وليست السلاح الذي نحارب فيه فدول مثل الهند واليابان وسنغافورة وماليزيا قامت ونهضت من خلال العلم لأنهم فهموا معنى الحرب ومعنى أن العلم هو من سوف يحكم الدول فيما بعد ولو أطلعت على تاريخ سنغافورة وأطلعت على الموارد التي لديها لبدأت البكاء على نفسك وعلى أمتنا العربية فنحن كدول نملك أكثر مما يملكون بأضعاف مضاعفة لكن أين نحن وأين هم ؟؟؟

عادة ماتصلي رسائل وردود تشكرني على العمل الذي أقدمه وتقول لي ياليت العالم العربي يملك مئة شخص يفكرون مثلما أفكر لتغيير وضعنا كثيرين وأنا اليوم أرد عليهم بشيء واحد لا تقول لي ياريت فأنا لأحب سماع هذه الكلمة لأنك لو فعلا فهمت وأيقنت بأن عملي كان فعلا جيد

التصميم والإخراج الفني

صدي

حلول تقنية متكاملة

eng.Anas kh al-Ahmad

eng.Salah Baybars

سوريا - دير الزور

00963 51 215452

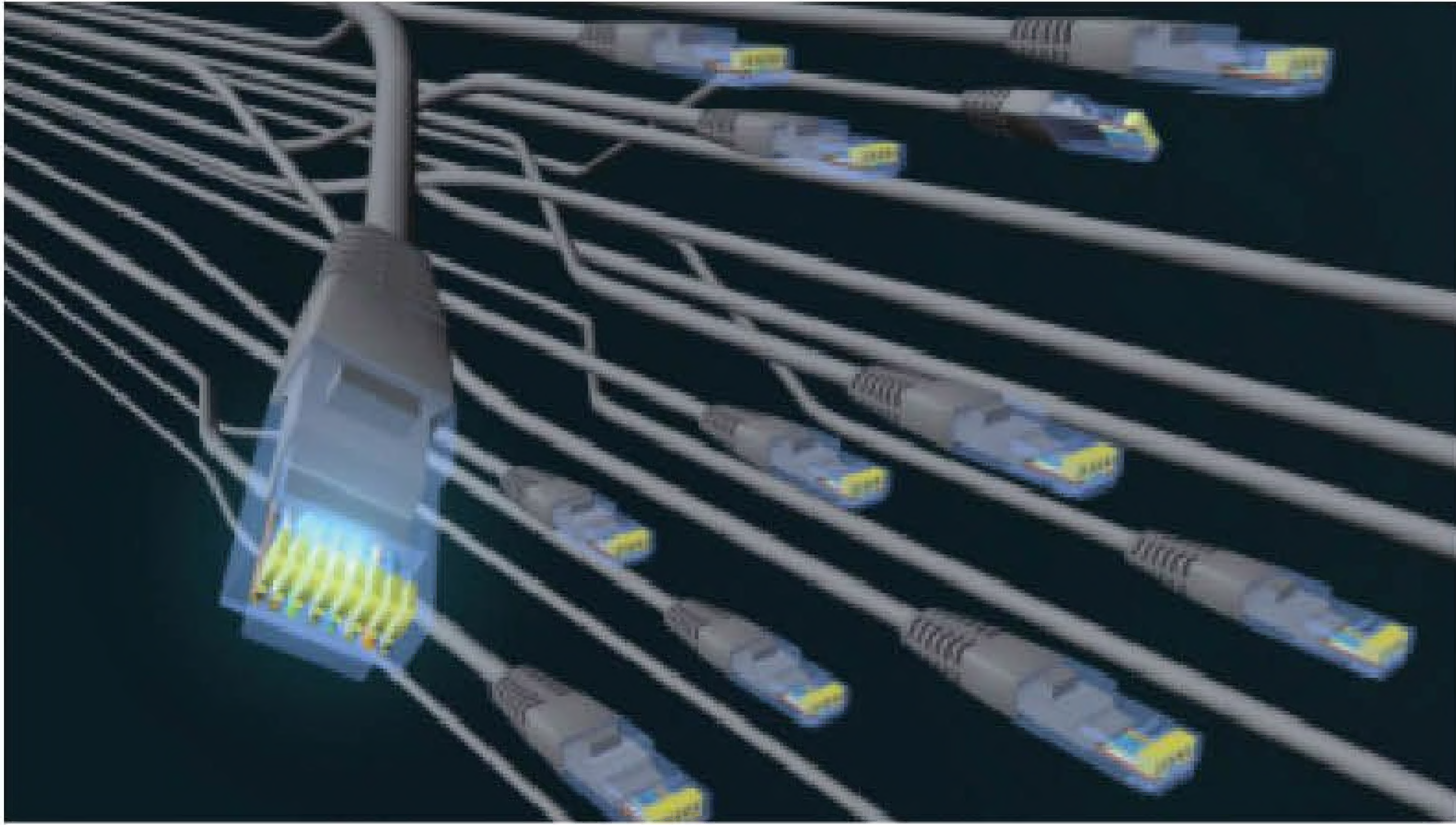
00963 967 962 665

الآراء المنشورة تعبر عن وجهة نظر الكاتب ولا تعبر عن وجهة نظر المجلة // جميع المحتويات تخضع لحقوق الملكية الفكرية // ولا يجوز النقل أو الاقتباس دون إذن من الكاتب أو المجلة

ملحوظة

المستويات

الصفحة	الموضوع
٣	المحتويات
٤	تعريف عملية حل مشاكل الشبكة والإجراءات التشخيصية
٦	DPM ٢٠١٠
١٠	منظمة الواى فاى و معاييرها
١٢	ثاني خطوات إحتراف علم ال Troubleshooting
١٦	الكابلات
١٨	Data Link Flow Control Protocols
٢٠	بداية الشبكات اللاسلكية
٢٢	Cryptography Part II Classical Encryption
٢٥	طريقة عمل call hunting
٢٨	Call Coverage





مفاهيم عامة في التفكير المنطقي

التحليل (analysis) هو عملية تقطيع بنية أو نظام إلى المكونات التي يتألف منها والعلاقة بينها.

عليك التفكير أولاً وقبل البدء في حل المشكلة، بأربعة أجزاء رئيسية (على الأقل) هي مكونات الشبكة، ولاحظ أن كل جزء من هذه الأجزاء مكون من عدة أجزاء:

1- مجموعة الأجهزة المدمجة في الشبكة (روتر - سويتش - سيرفر - مودم - كمبيوتر...).

2- نظم التشغيل للأجهزة السابقة وطريقة العمل عليها وإعداداتها.

3- التطبيقات والبرامج المستخدمة في الشبكة والتي قد تكون مصدر إزعاج لك.

4- المستخدمين حيث يجب أن تعرف أن المستخدم هو جزء معقد ومهم جداً من المشكلة.

نعم يتطلب الاصطياذ الفعال للمشاكل بعض الخبرة والخلفية العلمية لتحليل المشكلة الحاصلة، وإيجاد الحل الصحيح لها، بالسير على الخطوات التالية، لكنك أيضاً تحتاج إلى تذكر بعض الخطوات المنطقية الأخرى مثل: أن تسأل نفسك "هل هناك مشكلة؟". ربما المشكلة ناتجة عن أن الزبون (المستخدم العادي) يتوقع الكثير من الكمبيوتر وليس هناك مشكلة. وإذا كانت هناك مشكلة، هل هي مشكلة واحدة فقط، أو عدة مشاكل؟ وغيرها من الأسئلة ...

خطوات حل المشاكل:

الخطوة الأولى: تكلم مع الزبون

أحد المفاتيح للعمل مع الزبائن (سواء في نفس شركتك أم في شركة أخرى) هو ضمان تعاطيك بروية وحكمة معهم (تماماً كالطبيب). فمعظم الأشخاص ليسوا خبراء تقنيين مثلك، وعندما يحصل خطأ يرتبكون أو حتى يخافون أن اللوم سيقع عليهم. طمئنهم أنك فقط تحاول إصلاح المشكلة، لكن قد يمكنهم أن يساعدوا لأنهم يعرفون ماذا جرى قبل أن تصل إليهم. من المهم أن تجعل الزبون يثق بك. صدق ما يقوله الزبون، لكن صدق أيضاً أنه قد لا يقول لك كل شيء فوراً. ليس لأنه يكذب عليك، لكن فقط قد لا يعلم ما هي الأمور المهمة لكي يقولها لك.



قصة: إنها قصة كلاسيكية قد تبدو كنكتة، لكنها حصلت فعلاً. اتصل زبون بقسم الدعم التقني لأن كمبيوتره يرفض أن يشتغل. بعد 20 دقيقة من التحليل، أصبح التقني مُحَبَطاً... ربما المشكلة أن مزود الطاقة معطوب؟ فيطلب التقني من المستخدم أن يقرأ له بعض الأرقام على الجهة الخلفية لكمبيوتره، فيرد عليه المستخدم، "مهلاً، دعني أحضر شمعة. فالظلام دامس هنا لأن الكهرباء مقطوعة".

وهذه قصة حدثت لي شخصياً، كنت يوماً في أحد القاعات الذكية والتي تستخدم في الاجتماعات المرئية لأشخاص في مدن أو بلدان مختلفة أو ما يسمى بالفيديو كونفرنس، وكانت هناك مشكلة نريد حلها ثم ظهرت لنا مشكلة أخرى، وهي أن النظام غير متصل لا نستطيع الاتصال أصلاً بالقاعات الأخرى بالمدن المختلفة ولا حتى في نفس مدينتنا، مع أن الاتصال كان محققاً بالأمس ولكن كفاءة وجودة الاتصال كانت هي المشكلة، وظللنا نحاول مع الروتر والسويتش هل هناك خلل في الإعدادات أم الكيبلات أم البروجكتور، ثم قلت افحصوا كرت الشبكة الخاص بجهاز الكمبيوتر الذي يدير القاعة (السيرفر) وهنا كانت المفاجأة وما تخيلت أن الشخص المسئول والذي يقف بجانبنا ويرى حيرتنا، لم يقم بتشغيل جهاز الكمبيوتر هذا، وكانت هذه هي المشكلة.

ساعد في توضيح الأمور بجعل الزبون يبين لك ما هي المشكلة. أفضل طريقة رأيتهما لفعل ذلك هي أن تسأله، "أرني كيف يبدو الشيء الذي لا يعمل". بهذه الطريقة، ستري الظروف والأحوال التي تحدث فيها المشكلة. قد تكون المشكلة بسيطة بأن الزبون ينفذ طريقة غير ملائمة. قد يكون الزبون ينفذ عملية بشكل غير صحيح أو ينفذ الخطوات في الترتيب الخطأ. خلال هذه الخطوة، لديك فرصة لمراقبة كيفية حصول المشكلة، لذا انتبه جيداً وكن متيقظاً...

الخطوة الثانية: جمع معلومات

لقد حصل شيء بين الوقت الذي كانت فيه الشبكة تعمل والوقت الذي توقفت فيه عن العمل. عمالك كمتحري بوليسي بأدواتك هو معرفة ما هو ذلك "الشيء". اسأل المستخدم ما الذي تغير مؤخراً. هل أضفت جهازاً أو برنامجاً جديداً؟ هل تم نقل الكمبيوتر من مكانه؟ هل هناك شخص لا يستعمل الكمبيوتر عادة استعمله؟ هل وهل وهل؟ هذه هي أنواع الأسئلة التي يمكنك طرحها على المستخدم في محاولة لمعرفة ما الذي قد سبب المشكلة.

بالتحقيق أكثر، إعرف متى عمل الكمبيوتر لآخر مرة. هل حصل أي شيء خلال ذلك؟ هل يمكن إعادة التسبب بالمشكلة؟ (إذا لم يكن بالإمكان إعادة التسبب بالمشكلة، ستكون مشكلة لا يمكن إصلاحها). القصد هنا هو طرح قدر ما تحتاج من أسئلة من أجل تسليط الضوء

على المشكلة، ولا تنسى أن تجعل أسئلتك تغطي الأجزاء الأربعة للشبكة السابق ذكرها. إذا كانت الكهرباء مقطوعة في المنزل، كما في القصة التي رويتها لك سابقاً، فلا معنى عندها للمحاولة (إبتسامة)...

الخطوة الثالثة: استبعد الاحتمالات وضع الحلول ثم انتق منها بعدما تتضح المشكلة (المشاكل)، خطوتك التالية هي عزل الأسباب المحتملة، إذا كان لا يمكن التعرف على المشكلة بوضوح، ستحتاج إلى إجراء مزيد من الاختبارات والأسئلة. ابدأ باستبعاد الاحتمالات عليك معرفة المذهب الحقيقي وتبرئة ساحة الآخرين، الأجهزة أعني وليس المستخدمين.

تلميح: هناك أسلوب شائع لحل المشاكل وهو تجريد النظام نزولاً حتى أبسط مكوناته الأساسية. لمعرفة سبب المشكلة.

بعدما تستبعد كل الخيارات وتعزل المشكلة، ابدأ في تنفيذ أفضل ما تراه من الحلول، كأن تقوم بإعادة بناء النظام تدريجياً لترى إذا كانت المشكلة ستعود (أو تزول). هذا يساعدك على معرفة ما الذي يسبب المشكلة حقاً، وإذا كانت هناك عوامل مؤثرة أخرى.

تلميح: قبل بدء استبعاد الاحتمالات، افحص موقع البائع على الويب لأي معلومات قد تساعدك. مثلاً، كتابة رسالة الخطأ المحددة في موقع البائع قد تأخذك مباشرة إلى خطوات محددة لإصلاح المشكلة.

الخطوة الرابعة: قيم نتائجك

إذا نجح تصحيحك للمشكلة، تكون قد انتهيت ويمكنك الانتقال إلى الخطوة الخامسة. وإلا ستحتاج إلى إعادة التقييم والبحث عن الخيار التالي. إذا فقد جربت ولم يفلح، تابع وحاول الشيء المنطقي التالي.

عند تقييم نتائجك والبحث عن تلك "الخطوة التالية" الذهبية، لا تنسى الموارد الأخرى التي قد تكون متوفرة لديك. استعمل الإنترنت للبحث في موقع ويب الصانع. اقرأ كتيب الاستخدام. تكلم مع صديقك الذي يعرف كل شيء عن الأجهزة وإصداراتها. عند تصحيح المشاكل، يمكن أن يكون عقلان أفضل من عقل واحد.

الخطوة الخامسة: وثق عملك

الكثير من الأشخاص يستطيعون حل المشاكل. لكن المفتاح هو ما إذا كان يمكنك تذكر ماذا فعلت عندما حلت المشكلة منذ شهر. ربما. لكن هل يستطيع أحد زملاءك أن يتذكر شيئاً فعلته لإصلاح نفس المشكلة في تلك الآلة منذ شهر؟ غير محتمل. دائماً وثق عملك لكي تستطيع أنت أو أي شخص آخر أن تتعلم من تلك التجربة. بإمكان الوثائق الجيدة لحلول المشاكل السابقة أن توفر ساعات من الإجهاد في المستقبل.

سيناريو واقعي: وثق كل شيء!

أحد الأشياء التي أوصي بها دائماً التقنيين الجدد هو شراء دفتر ملاحظات وحمله معهم أينما ذهبوا. نوع دفتر الملاحظات لا يهم حقاً، لكنني أفضل النوع اللولبي (لإبقاء الأوراق آمنة) مع كثير من الصفحات (لأنك ستستعمل الكثير منها).

كلما صادفك مصطلح لست معتاداً عليه، دوّنه. يمكنك البحث عن معناه لاحقاً عندما يكون لديك وقت ووصول إلى موارد أكثر. إذا كنت تحاول إصلاح مشكلة، دوّن رسائل الخطأ بشكل دقيق. وثق تماماً كل خطوة تقوم بها في تصحيح المشكلة. السبب والتأثير: ماذا غيّرت وماذا حصل عندما غيّرت؟ أحياناً الجواب "لا شيء تغير" يساعدك على استبعاد الأسباب المحتملة للمشكلة.

عندما تبدأ، سيكون دفتر الملاحظات هذا لا يُقدّر بثمن. لن يتضمن الكثير من التنظيم على الأرجح، والعديد من الأشياء التي تكتبها قد تجد صعوبة في قراءتها لاحقاً. لكن تلك الملاحظات ستساعدك. بمقدار كبير عندما تحتاج إليها لأن لا أحد يستطيع أن يتذكر كل شيء. خاصة عندما تكون جديداً في أحد الأشياء.

في نهاية المطاف قد يقل اعتمادك على دفتر الملاحظات رويداً رويداً، لكن لا يزال من الجيد إبقائه بمتناول اليد. نظمه بطريقة تناسب احتياجاتك، وستجد أن بإمكانه أن يكون أفضل أداة لحل المشاكل.

تعريف الموارد التشخيصية:

بالإضافة إلى الأدوات التشخيصية العديدة المتوفرة لك، هناك بعض الموارد التشخيصية التي يجب أن تستعملها لتسهّل عملية اصطلياد المشاكل. رغم أن معظم الأشخاص لا يعتبرون بالضرورة أن تلك الموارد هي أدوات، إلا أنها تساعد في عملية اصطلياد المشاكل.

تلك الموارد تتضمن:

• الكتيبات.



• موارد الإنترنت.

• مواد التدريب.

كتيبات المستخدم/ التثبيت

التقنيون هم أكثر الأشخاص الذين لا يستعملون هذا المورد المتوفر بسرعة عند محاولتهم حل مشكلة في الشبكة. في الواقع، يتكل التقني معظم الأحيان على خبرته ويحاول تثبيت مكوّن جديد من دون قراءة الكتيب. ثم، عندما لا يعمل التثبيت، قد يلجأ إلى الكتيب بعد أن يكون قد قضى وقتاً لا بأس به في البحث عن حل لمشكلة ربما كان من الممكن تجنبها من البداية. عادة، بالإضافة إلى الخطوات المطلوبة لتثبيت برنامج أو جهاز، يتضمن الكتيب قسماً عن المشاكل الأكثر شيوعاً والحلول لتلك المشاكل. هذه الناحية في الكتيب مفيدة بشكل خاص للتقني الذي وصفناه للتو.

موارد الإنترنت/ الويب

ربما المورد الأكثر فائدة للتقني هو الإنترنت. كما هو مذكور طوال هذه المقالة، موقع ويب الصانع هو أفضل مكان للحصول منه على أحدث التحديثات والنصائح



والتصحيحات والمعلومات التقنية. في أغلب الأحيان، يمكنك البحث في موقع ويب بائع الجهاز أو البرنامج عن مشكلة قد تعاني منها في ذلك الجهاز أو البرنامج، وستجد حلاً لها. بالإضافة إلى ذلك، عليك بزيارة قسم الدعم الفني Support بالموقع. إذا لم تكن تستطيع إيجاد جواب في موقع الصانع يمكنك محاولة كتابة مشكلتك في أشهر وأقوى محركات البحث العم جوجل وهو سيساعدك حتماً.

هناك أيضاً مواقع ويب مخصصة لمجتمعات من الأفراد التقنيين (مثلك أنت) تعرف بالمنتديات مثل عرب هاردوير وبوابة العرب التعليمية وسيسكو التعليمي وغيرها الكثير، وهذه المواقع يمكنها أن تكون مصدراً رائعاً للمعلومات. هناك احتمال كبير إذا كنت تعاني من مشكلة في الشبكة أو مشكلة تقنية أن هناك شخصاً آخر، في مكان ما في العالم، لديه الحل - ويمكن للإنترنت أن تجمعكما سوية. يمكنك أيضاً نشر مشكلتك في أي عدد من المنتديات أو المجموعات على الويب ثم تلقى الجواب، وربما في غضون دقائق.

مواد التدريب

المورد الأخير هو واحد يتغاضى عنه معظم الأشخاص. لا يكتسب الأفراد العلم والمعرفة من عدم - فهم إما يتعلمونها بأنفسهم بواسطة مواد التدريس الذاتي، أو يتعلمونها من مدرس خبير. في كلا الحالتين، الكتب ومواد التدريب الأخرى هي مصادر ممتازة للمعلومات. رغم أن مواد التدريب لا تحتوي في أغلب الأحيان على تصحيحات أو تحديثات، إلا أنها ستعلمك مفاهيم يمكنك تطبيقها لتساعدك في اصطيات المشاكل. ففي النهاية، لو أنك لم تقرأ تلك المقالة، لما كنت حصلت على الخطوات التي تحتاج إليها لتحل مشاكلك.

الآن اسأل نفسك: هل تعلمت شيئاً؟ هل المعلومات التي تعلمتها ستكون قادرة على مساعدتي في حل مشاكل الشبكة؟

تنفيذ الصيانة الدورية والوقائية ومراقبة الأنظمة والشبكة:

حقيقة لا أحب أن أطيل عليك أكثر من ذلك، لكن ما أردت أن أقوله في هذه الجزئية وهي من الأهمية بمكان، أن هناك في الحقيقة عدد مرعب من الأسباب التي قد تسبب انهيار الأنظمة والشبكة، لكن تلك الانهيارات لا تحصل في أغلب الأحيان في ظروف عادية، وهذا ما قد يجعلك تطمئن نسبياً. لكنك تلعب دوراً مهماً في استقرار الأنظمة والشبكة وذلك بتنفيذ الصيانة الدورية والوقائية وإجراء عمليات المراقبة المستمرة. وإذا أهملت المحافظة على ذلك فيمكن أن تكون هناك مشكلة كبيرة بانتظارك في المستقبل ستؤثر على إنتاجيتك وبالتالي مستقبلك أو إنتاجية الأنظمة والشبكة لديك.

وفي النهاية أرجو أن تكون وصلتك الإجابة عن سؤال في أول المقال عن الدور الرئيسي لرجال الشبكات ألا وهو حل المشاكل Troubleshooting نعم المشاكل اليومية والتي تحدث نتيجة الاستخدام السيئ من قبل المستخدم العادي Users وهذا أغلبها أو نتيجة تطبيق (برنامج) أو نظام تشغيل أو كيا بل أو سيرفرات أو هاردوير (سويتش روتر) قديم أو قالف وهذا الأخير أندرهما. وبهذا أرجو أن أكون وضعت لك منهجية تسير بها في حل مشاكلك اليومية آسف أقصد دورك الوظيفي بشكل سلس ومرتب وفاعل.

ملحوظة: أنصح بقراءة المقالة أكثر من مرة وتلخيص الخطوات والإجراءات وابدأ من الآن وجرب أن تتعامل وتتصرف مع مشاكل الشبكة كالخبراء والمحترفين لا كالمبتدئين.



Microsoft® System Center Data Protection Manager

بتاريخ 2010/2/8 أعلنت مايكروسوفت عن طرح نسخة المستخدم الـ "RC0" لنظام الحماية "DPM2010" الجيل الثالث والذي كان يعرف مسبقاً بـ "DPM v3" أو "Zinger".

الهدف من هذا النظام هو عمل النسخ الاحتياطي (سواء على الهارد دسك او باستخدام الاشرطة "Tape") وخطط الطوارئ لمختلف انظمه مايكروسوفت اضافته الى الملفات وقد تم اضافته عدة تحسينات في الاصدار الحالي بحيث اصبح بالامكان الان حمايه الانظمه الاتيه وعمل نسخ احتياطي لها:-

- Windows Server from 2003 through 2008 R2
- SQL Server 2000 through 2008 R2
- Exchange Server 2003 through 2010
- SharePoint Server 2003 through 2010
- Dynamics AX 2009
- Essential Business Server 2008 and Small Business Server 2008
- SAP running on SQL Server

اضافه الى دعم الاجيال الجديده من انظمه مايكروسوفت سيرفر ، التحسينات الجديده شملت:-

- امكانيه حمايه 2000 قاعده بيانات SQL من خلال سيرفر DPM واحد ، ونوعيه النسخ الاحتياطي هي نسخه السيرفر بحال لو فشل السيرفر في عمليه الاقلاع يمكن عمل Restore لاعادته الى وضعه الطبيعي وعمليه نسخ البيانات بحيث يمكن اعاده قواعد البيانات فقط، مع ملاحظه ان جميع القواعد الجديده ستتم حمايتها ذاتيا.
- مدراء الـ Sharepoint ايضا سيلاحظون امكانيه حمايه محتويات قواعد البيانات الجديده ذاتيا بصورة كامله بدون الحاجه الى استثناء سيرفرات الـ 14 والتي كانت تتم حمايتها بصورة مستقله.

اضافه الى ماورد اعلاه فلنظام الحماية قدرات جديده في حمايه منتجات مايكروسوفت ضمن بيئه Virtualization وكالاتي

- Microsoft Virtual Server 2005 R2
- Windows Server 2008 with Hyper-V
- Windows Server 2008 R2 with Hyper-V
- Hyper-V Server 2008 and 2008 R2
- Protection of Live Migration-enabled servers running on CSV in Hyper-V R2

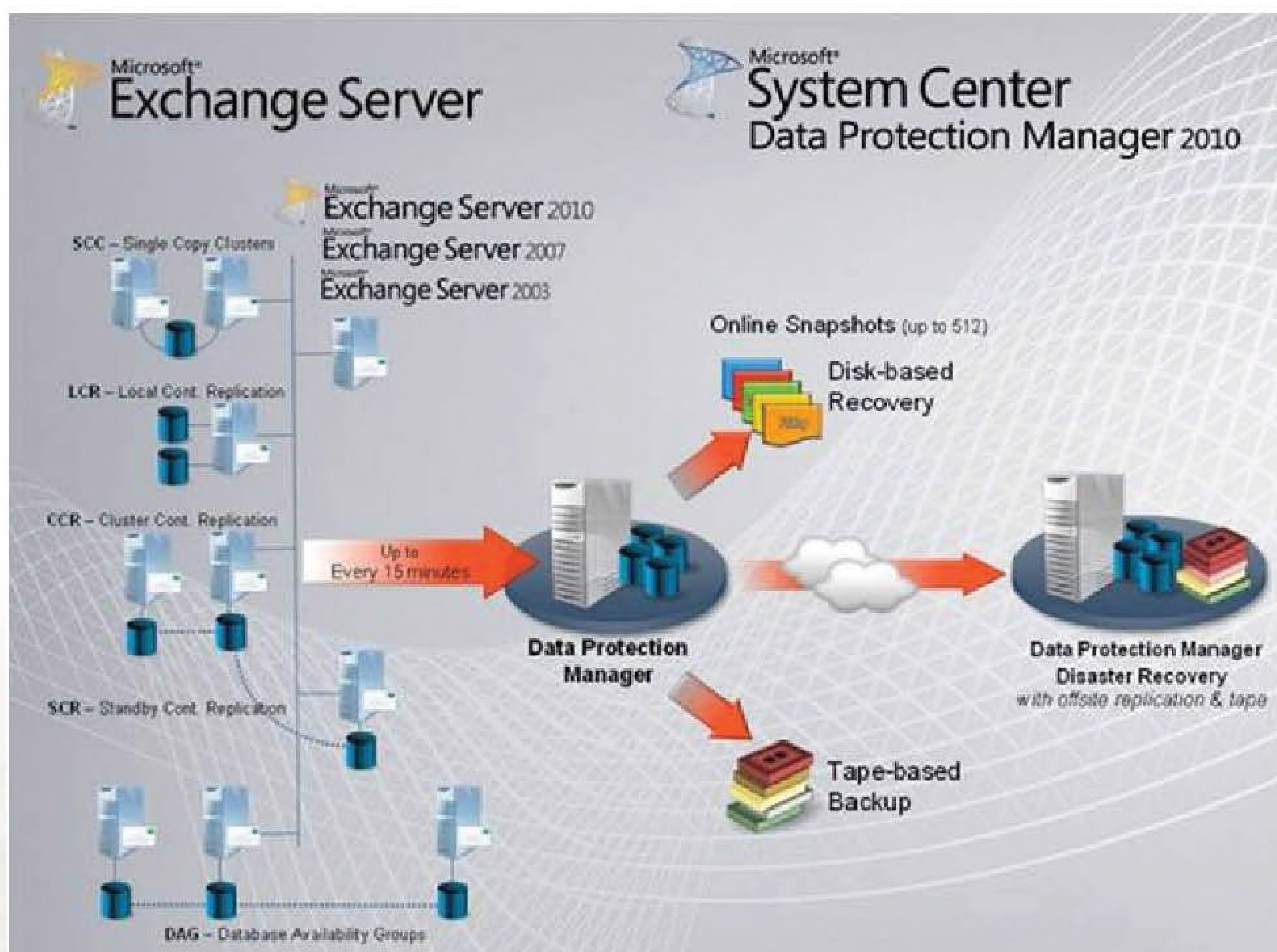
• امكانيه حمايه الاجهزه الوهميه من الوندوز المستضيف او من مستضيف الهايبرفايسر Hypervisor.

• Host-based backups will now enable



Microsoft®
System Center
Data Protection Manager 2010

- single-item restores from within the VHD
- امكانيه عمل Restore لجهاز وهمي Virtual على مستضيف اخر.
- حمايه المستخدمين
- حمايه الانظمه من وندوز اكس بي الى وندوز 7.
- اداره مركزيه للبولسي في DPM2010 ، فبينما اجهزه الاب توب هي online او offline "مربطه بالشبكه او لا" ، يتم عمل نسخ احتياطي من خلال اداره البولسي الخاصه بـ VSS client/backup tools.
- Restore يتم ايضا من سواء كان الجهاز online او لا من خلال عمل Restore وفرض تناقل الملفات الى الكمبيوتر فور اتصاله.
- التحقق من جوده عمليه النسخ الاحتياطي من خلال مراجعه البيانات والتأكد من صحه طريقه تخزينها.
- حمايه البيانات ضمن بيئته Clustering بامكان الـ DPM2010 حمايه البيانات في الحالات التاليه
- SCC - Single Copy Cluster ، وهو حينما يرتبط جهازي سيرفر بوحده خزن من نوع SAN.
- LCR - Local Cont. Replication ، حينما يرتبط سيرفر بوحده خزن من نوع SAN.
- CCR - Cluster Cont. Replication ، حينما يرتبط كل سيرفر بوحده خزن من نوع SAN ويكون هنالك تكرار Replication بين وحدتي الخزن.
- SCR - Standby Cont. Replication ، حينما يرتبط سيرفر بوحده خزن من نوع SAN ويرتبط ايضا بعلاقه مع اجهزه اخرى من نوع CCR.
- DAG - Database Available group ، حينما ترتبط الاجهزه فيما بينها باكثر من نوع علاقته واحد مما ورد ذكره اعلاه.
- الشكل الاتي يوضح انواع العلاقات التي بوسع الـ DPM2010 التعامل معها
- التوسعات، الاعتماديه. الاداره
- حمايه 100 جهاز سيرفر، 1000 جهاز محمول، او 2000 قاعده بيانات بواسطه سيرفر DPM واحد.
- حمايه ذاتيه ، اعاده البيانات الى وضعها الاصلي في حال حصول اي اخطاء ذاتيا ، بالنتيجه تقليل نسبه التثنيه او الحاجه للتدخل من قبل مدير الشبكه.
- تحسين اداء حمايه الانظمه لفترات اطول وتحسين اداء تكامل الانظمه "خاصيه العلاج التلقائي Auto-healing".
- الملاحظات
- في بيئته تعتمد على انظمه مايكروسوفت قد يكون هذا النظام هو الحل الامثل مقارنة باسعار تطبيقات حمايه اخرى.
- مرونة النظام التي تتيح اعاده ملف واحد او نظام بأكمله الى حالته الطبيعيه.
- امكانيه اعاده البيانات الى مواقع بديله كاجهزه اخرى ونفس الحال ينطبق على الانظمه حيث بالامكان عمل نسخه نظام لجهاز سيرفر واعادتها الى سيرفر ثاني.
- مر و نه
- العمل بين عدة مواقع حيث ترتبط اجهزه الـ DPM2010 فيما بينها وبالامكان ادارتها جميعا من موقع واحد.
- في التقارير
- يستفاد النظام من تواجده SQL داخل الشبكه لحفظ المعلومات تمهيدا لاصدار التقارير ، ويحال عدم تواجده نسخه SQL فيسمح النظام بتنصيب نسخه SQL



DPM Primary Backup Requirements Calculations Pane	
Backup Config Params	
Effective Backup Connection Throughput / VM	20 MB/s
Effective Restore Connection Throughput / VM	30 MB/s
Max parallel backups possible per Hyper-V Node	6
Max parallel backups possible per DPM server	12
Number of parallel backups	12
DPM Primary Backup Requirements Results Pane	
If any of the cells in this sheet are RED, either read the text, or hover over the cell and read the comment. This will provide you with the information to manage the issue.	
Hyper-V Server Configuration	
Total Number of VMs in the Hyper-V Cluster	12
Number of Hyper-V servers protected	10
Number of VMs per Hyper-V Node	1
Max Number of parallel backups / Node**	8
Max Number of parallel backups / CSV**	4
** Refer to DPM documentation for Hyper-V on how to work with these numbers.	
Hardware: DPM Number of Servers & Total Storage	
Number of DPM Servers	1
Replica Volume Size /VM	250 GB
Recovery Point Volume Size /VM	107 GB
Total Replica Volume Size	3000 GB
Total Recovery Point Volume Size	1279 GB
Total Storage Required	4.18 TB
Hardware: DPM Server & Storage Requirement	
Recommended Number of Processor Cores / DPM Server	4
Recommended RAM Configuration / DPM Server	12 GB
Recommended Page File / DPM Server	15 GB
Server Architecture	64 bit
Replica Volume Size	3000 GB
Recovery Volume Size	1279 GB
Total Storage per DPM Server	4.18 TB
Hardware: DPM Database Space Requirements	
Disk 1 for DPM SQL DB	10 GB
Disk 2 for DPM Logs	1 GB

DPM Configuration: Protected Group Configuration Data / DPM Server				
Protected Group	VM Grouping	Synchronization	Retention Range	Backup Window
PG1	VM1-VM12	Once/day	14 days	1Hrs

SLA: DPM Backup Time	
Time taken for Initial Replication of all VMs	1Hrs
Amount of data transferred / Backup period	90 GB
Time taken to Backup a VM	50 Mins
Time to Restore a VM	28 Mins
Time to Recover a Hyper-V Node	1Hrs

Note: The maximum number of DPM servers per Hyper-V cluster should always be 1, because VMs cannot be migrated between DPM servers.

If more than one DPM server is indicated, then you have the following options:

- Increase the input colocation factor (in the Input tab)
- Consider splitting the CSVs to be protected into several smaller clusters
- Reduce the number of input VMs that are protected
- Reduce the Retention Range

- نظام الحماية شامل لجميع منظومات المايكروسوفت بمعنى لاجابه لتطبيقات نسخ احتياطي اخرى في اي حال من الاحوال.
- بالامكان اعاده الملفات او الانظمه الى حالتها بالاعتماد على النسخ المتوفره وكما هو موضح في الشكل الاتي

The screenshot shows the DPM 2010 Administrator Console interface. The main window is titled "DPM 2010 Administrator Console" and has a menu bar with File, Action, View, and Help. Below the menu bar are tabs for Monitoring, Protection, Recovery, Reporting, and Management. The Recovery tab is active, showing a "Browse" and "Search" section. The "Protected data:" section shows a tree view of protected data, including "companyabc.com" and "FILE1". The "Recovery points for: C:\\" section shows a calendar for January 2010 with recovery points highlighted. The "Available recovery points are indicated in bold on the calendar. Select the date from the calendar and the time from the drop down list for the recovery points that you want. Click recover in the Actions pane to open the Recovery Wizard." section shows a "Recovery date:" of January 06 2010 and a "Recovery time:" of 6:00 PM. The "Recover from:" section shows a "Disk" icon. The "Path:" section shows "C:\Shared\". The "Search list below" section shows a table of recoverable items with columns for Recoverable Item, Last Modified, and Size. The table lists various folders and files, including "Marketing", "Sales", "IT", "Sales Update 345.docx", "Oh no!.docx", "Getting Started - You just took over...", "World Dom Plans (Do not read).docx", "Sales update 123.pptx", "Client One.pptx", "Read Me.docx", "Do you really look at this.pptx", "Super Cool Document.ppt", "Buy my book.ppt", and "Roadmap 2009-2010.ppt". The right-hand pane shows the "Actions" menu with options like "Microsoft System Center Data...", "View", "Help", "Selected Item", "Recover...", "Show all recovery points", "Verify data", "Configure end-user recovery...", "Options...", and "Help".

في عالم اليوم الذي يتضمن وفره في التطبيقات وزياده في تعقيد الشبكات واداء المهام يتم الانتقال تدريجيا الى وحدات السيطره المركزيه لاداره الاعمال وكما يبدو فان مايكروسوفت تسيير على نفس السياق ، هذا النظام سوف يريح الجوله في النهايه بالاعتماد على رخص الثمن مقارنة مع التطبيقات الاخرى ورغم انه الى الان ينصح به في الشبكات المتوسطة الا ان السنوات اللاحقه ستشهد مزيد من التطور مما يعني ان الوقت قد حان لالقاء الضوء بصورة اكبر على هذا النظام.

تستطيع أن تشترك في مجتمع الواي فاي من خلال هذا الموقع كي تكون على تحديث دائم لهذه التكنولوجيا، وكي تستطيع أن تخاطبهم رسمياً أيضاً عند إحتياجك أو عند مقابلتك أى مشاكل عند التعامل مع هذه التكنولوجيا.

لكي تقوم منظمة الواي فاي بإعتماد منتج معين فإنها لا بد أن تمرره خلال ثلاث مراحل:

المرحلة الأولى: التوافقية و هي مرحلة التأكد ما إذا كان المنتج سيتعامل بطبيعية مع أى منتج آخر شبيه من شركة أخرى أم لا.
المرحلة الثانية: مرحلة التوثيق أى إختبار إعداداته النظرية المعتمدة على ميثاق 802.11 وذلك لمعرفة ما إن كان سينجح فيزيائياً في التعامل مع الأجهزة الأخرى في نفس النطاق أم لا وهل سيعطى النتائج الصحيحة طبقاً للمعطيات التي طبقت عليه أم لا.
المرحلة الثالثة: مرحلة الأداء و هي إختبار مدى نجاح المنتج في إعطاء أقل أداء متوقع وغالباً ما يتم التأكد من ذلك من خلال المستخدمين أنفسهم حيث تعتبر مرحلة كمالية بالنسبة للمنتج وهو الشيء الذي يفرق بين المنتج المبني تكنولوجياً وفيزيائياً بدرجة صحيحة ولكنه يعتبر تصنيعياً رديئاً أو جيداً.

معايير منظمة WIFI

علي عكس معايير IEEE فإن wifi معاييرها متكاملة ليست تطويرية تلغى بعضها أي أنها كالخصائص التي تتوفر في جهاز معين و ليست متضاربة، و كلما توفرت إحدى هذه المعايير في جهاز كلما كان أفضل أداء و أعلى سعراً.

Wi-Fi Multimedia (WMM) certification

أصبحت الشبكات اللاسلكية من الشبكات التي يعتمد عليها في نقل البيانات وهذا مما يجعل البعض ليخاطر بنقل بيانات ذات صفة حرجية و أعنى بالبيانات ذات الصفة الحرجية هي البيانات التي لا تتطلب تأخر في الوصول أو وقوف في طوابير الإنتظار اعتماداً على خلو القنوات أو اعتماداً على الكثافة المرورية في الشبكة.
من هذه البيانات ذات الصفة الحرجية المكالمات الصوتية عبر الإنترنت، و طلبات تحويل الأموال و الحجوزات الفورية. هذا يسمى في عالم الشبكات QoS = Quality of services ، وهو باب ضخم جداً من أبواب الشبكات له دراسات خاصة به ومناهج متخصصة فيه و شهادات أيضاً.

ولهذا قامت المؤسسة المسؤولة عن الواي فاي wifi alliance بصنع

Wi-Fi Multimedia (WMM) certification

معيار و علي أساسه و وضعت بنود لأولوية البيانات في المرور في الشبكة و هي كالآتي:

Voice و هي البيانات التي تحمل صفات صوتية مثل المكالمات الهاتفية.

Video البيانات المرئية مثل التراسل المرئي و بيانات التلفاز عبر الإنترنت.

Best effort مهام التصفح و باقى البيانات غير ما سبق.

Background تطلق على المهام العادية للشبكة مثل تحميل ملف أو رفعه أو طباعة ملف ما.

wifi alliance هو مجتمع تقني غير ربحي يملك حصرياً العلامة المسجلة المسماه في عالمنا wi-fi وتختص بتكنولوجيا الشبكات اللاسلكية للشبكات المحلية أو WLAN وهو الجزء المسمى



IEEE 802 في هيئة IEEE التي تكلمنا عليها سابقاً. لم تتعد هيئة IEEE كونها منظمة لإعطاء المقاييس للأجهزة الكهربائية والإلكترونية، ولم يكن من إختصاصها إختبار الأجهزة التي تصنع طبقاً لهذه المقاييس لذلك كان على كل تخصص من تخصصات الكهرباء والإلكترونيات أن يقوموا بنفسهم بهذا الأمر. ولذلك فإنه في عام 1999 قامت العديد من الشركات المتخصصة في تصنيع الأجهزة اللاسلكية المعتمدة على تقنية الواي فاي بتجميع أنفسهم ضمن كتلة واحدة سموها wi-fi alliance وبلغ عددهم الآن 300 عضو في أكثر من 20 دولة.

قامت هذه المنظمة بضبط و دعم مواصفات آلاف الأجهزة وسواء كنت مدير في قطاع تكنولوجيا المعلومات أو مهندس أو فني أو حتى مستخدم عادي فلا بد أن تحتاج يوماً للبيانات والوثائق التي تكتبها وتدعمها هذه المنظمة لتستطيع التعامل مع أجهزتك اللاسلكية. فبالإضافة إلى أن تلك المنظمة تقوم بوضع الأسس التكنولوجية للواي فاي وإختبارها فإنه على عاتقها عمل تحديث دوري لتلك التقنيات ودعم السوفت وير الخاص بها و الإهتمام بالحالة الاقتصادية للمنتجات. و عموماً أى شيء يخص المنتج اللاسلكي «واي فاي» فإنه لا يخرج عن نطاق هذه المنظمة، و لذلك فإنه عند وجود منتج يدعم منظمتي IEEE و wifi فإنك تجد هذا الشكل:



Wi-Fi Alliance WMM Power Save Certification

كانت أكبر مشكلة تواجه دعم تقنية الواي فاي في الأجهزة المحمولة مثل الموبايل و اللابتوب و البالم توب و غيرها هي الطاقة فمن البديهي أنه زيادة خاصية مثل الواي فاي في تلك الأجهزة سيجعلها تستهلك طاقة أكثر مما يجعل فترة الاستفادة من شحن البطارية أقل. ولهذا قامت المؤسسة المسؤولة عن الواي فاي بعمل مقياس لهذا الأمر و أطلقت عليه Wi-Fi Alliance WMM Power Save Certification وقد أدرج هذا ضمن المقياس الرئيسي IEEE 802.11e.

ولقد أصبحت الشركات تتبارى في دعم هذه الخاصية ومن أوائل المنتجات التي دعمت هذا الأمر كما ذكرته مؤسسة Wi-Fi (WPS (Wi-Fi Protected Setup



هو مقياس لإعداد الشبكات اللاسلكية بوجه آمن و ميسر أنشئ من قبل Wi-Fi Alliance و بعض المؤسسات في (٨ January ٢٠٠٧) لجعل إعداد الشبكة اللاسلكية أكثر أمنا و يسر، و قد كان إسم المقياس أولا Wi-Fi Simple Config فكما هو معلوم أنك تبدأ بوضع أجهزتك ثم تقوم بإعطاء شبكتك مسم SSID، و تقوم بإعداد سياسة الأمن لديك حسب ما تفضله أو ما هو مدعم لدى أجهزتك من طرق التشفير و التوثيق.

و في WPS يقوم صاحب أو مدير الشبكة بإختيار أحد هذه الطرق للتواصل مع موزع الإشارة اللاسلكية access point و كلها تعتمد أولا على تسجيل وجودك في محيط الشبكة لتستطيع نيل خدماتها.

طرق تشفير الشبكات اللاسلكية

Wi-Fi Protected Access (WPA/WPA٢) certification



قامت منظمة الواي فاي بدعم طرق تشفير و ذلك لحماية تدفق البيانات في الشبكة اللاسلكية و هو أمر شرحه يطول، و سنتكلم عنه في مقالات خاصة به.

نادر المنسي

6 Method

- The Top-Down
- The Bottom-Up
- The Divide and Conquer
- Following the Traffic Path
- Comparing Configurations
- Component Swapping



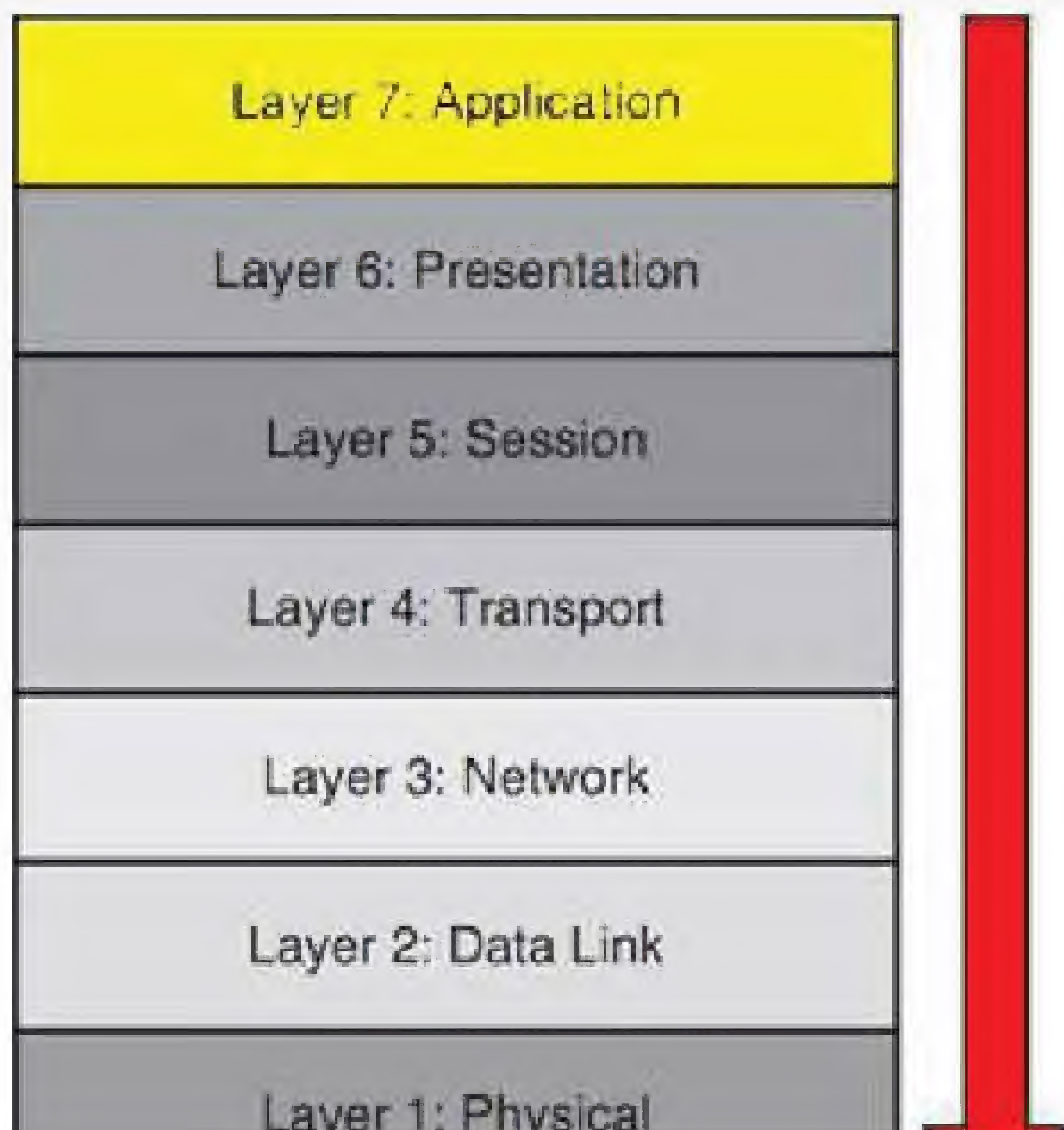
من أن كل طبقة تعمل بشكل صحيح وفي مثالنا هذا سوف نتوجه إلى الـ Transport Layer للتأكد من أن المنفذ 80 وبروتوكول الـ TCP يعملان بشكل صحيح وهكذا إلى نبدأ برسم معالم المشكلة بشكل أكبر.

أستكمالا لما بدأناه حول أولى طرق احتراف علم الـ Troubleshooting نتابع اليوم معكم تقديم الخطوة الثانية في احتراف هذا العالم والتي سوف أخصصها للحديث عن الطرق والأساليب المتبعة في إنقاص نسبة الاحتمالات المسببة وبالانكليزية Troubleshoot Approaches

عادة عندما نواجه مشكلة ما في الشبكات نبدأ حلها باتخاذ بعض الخطوات والتي بدورها تساعدنا على إنقاص نسبة الاحتمالات المسببة لهذه المشكلة وتختلف هذه الخطوات بحسب خبرة الشخص ونوعية المشكلة واليوم سوف نتحدث عن هذه الطرق والأساليب المتبعة وهي بشكل عام ستة طرق :

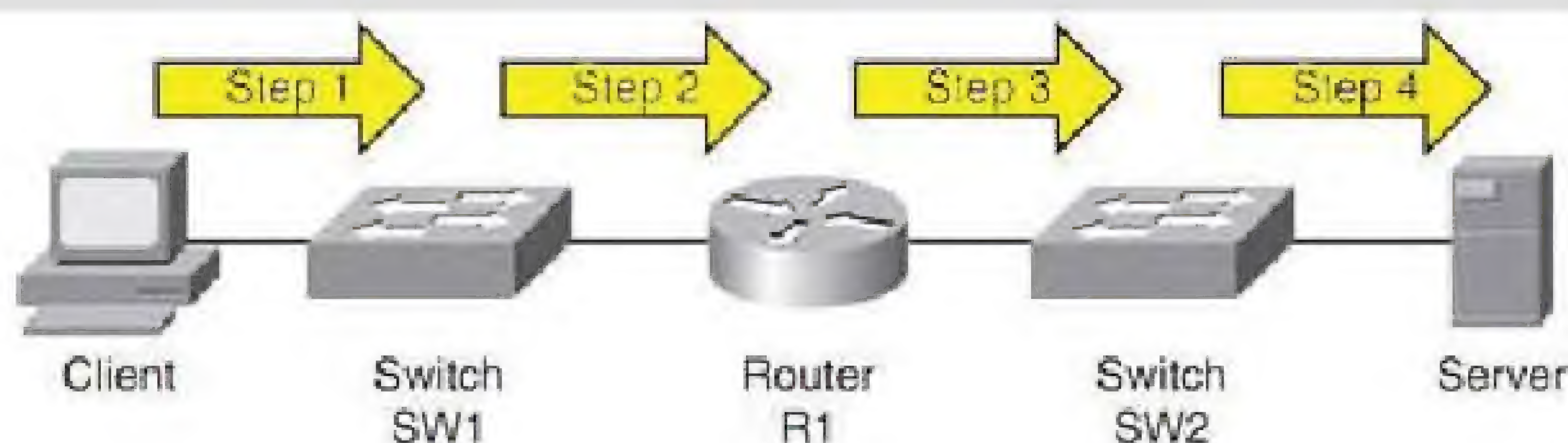
The Top-Down Method

تعتبر الطريقة الاولى أحد الطرق التي تعتمد على الـ OSI Layer والتي تبدأ في طبقة الـ Application Layer وتتجه للأسفل لذلك أطلق عليها أسلوب الأعلى الأسفل ويعتبر هذا الأسلوب أحد الأساليب المعروفة في حل المشاكل فهو يعتمد على مبدأ فحص الأسباب من خلال فحص الطبقة الأعلى نزولاً إلى آخر طبقة ولكي أقرب لكم الفكرة لنأخذ مثالا واقعيا : يتصل بك أحد الأشخاص ويخبرك بأن لديه مشكلة مع الأنترنت ؟ عندما نبدأ حل المشكلة باستخدام هذا الأسلوب نبدأ بتفحص الـ application نفسه ونحاول التأكد ان المتصفح سليم وبأن المشكلة ليست منه وبعدها نتجه إلى باقي الطبقات ونحاول التأكد



Following the Traffic Path

تتبع المسار وهو أسلوب مفيد وبسيط نوعا ما وهو يساعد في تحديد المكان أو Area للمشكلة وذلك من خلال تتبع مسار مرور الباكيت، وصولا إلى هدفها وكمثال بسيط لنفرض أن هناك مشكلة بين سيرفر ومستخدم وبينهم هناك سويتش وروتر. نبدأ خطوات حل المشكلة بفحص الكابل بين المستخدم والسويتش وبعدها نتأكد من الإتصال بينهم وبعدها نفحص الكابل بين الروتر والسيرفر ونتأكد من وجود إتصال بينهم، وهكذا إلى أن نستطيع رسم أولا خطوات تحديد المشكلة.



Comparing Configurations

يعتبر هذا الأسلوب من أبسط وأسهل الأساليب التي تستخدم لتحديد المشاكل والتي عادة ما يستخدمها المبتدئين، ويمكن تشبيه هذه الطريقة باللعبة التي نشاهدها على بعض أقنية النصب والإحتيال على التلفاز حول تحديد نقاط الاختلاف بين صورتان وأكد الذي يستطيع تحديد أماكن الاختلاف يربح مئة ألف دولار !. المهم هذا الأسلوب يعتمد على نفس الفكرة من خلال مقارنة الإعدادات الموجودة على مكان آخر، وكمثال بسيط نفرض أن هناك روتر لا يعمل أو هناك مشكلة تقنية والحل أن نقوم بعمل مقارنة بين نسخة إعدادات سابقة لنفس الروتر مع الإعدادات الحالية أو أن نقوم بمقارنة الإعدادات الموجودة على روتر آخر يقوم بنفس العملية التي يقوم بها، أو أن يكون لدينا جهازان كمبيوتر واحد يدخل على الإنترنت والثاني لا، والحل أن نقوم بمقارنة إعدادات الجهاز الذي يعمل مع إعدادات الجهاز الذي لا يعمل الأول لإكتشاف نقاط الاختلاف بينهم وهذا يشمل الأيبيات والجدار الناري، والجيت واي، وإعدادات المتصفح وإلخ....

Component Swapping

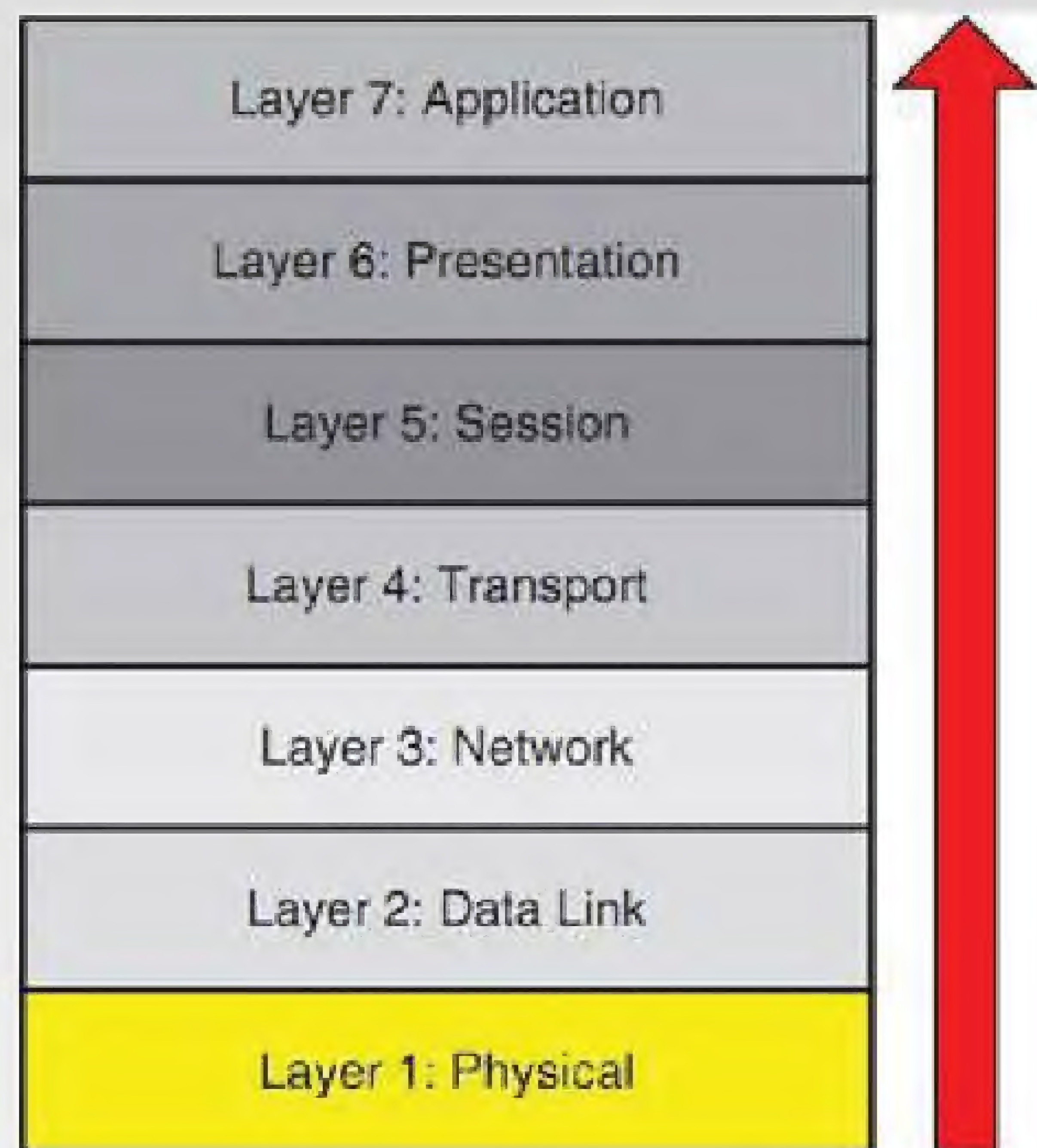
الطريقة السادسة والأخيرة تعتبر أيضا خاصة بالمبتدئين أمثالي ولكن فعالة نوعا ما برأيي وهي تعتمد على تبديل العناصر التي تسبب هذه المشكلة، وكمثال بسيط لنفرض أن لدينا مشكلة بين جهاز وسويتش نقوم أولا بتغيير الكابل مع كابل آخر لكن بشرط أن نكون متأكدين من أن الكابل الجديد يعمل لذلك يفضل استخدام كابل مجرب وليس جديد تماما، ولو كانت النتائج سلبية أيضا نقوم بإستبدال السويتش بسويتش آخر وبعدها نستبدل الكمبيوتر وإلخ.... إلى أن نصل إلى تحديد معالم هذه المشكلة.

أتمنى أن تكونوا قد إستفدتم من الأفكار المطروحة في هذا الموضوع فهي بدائية لكن يجب علينا أن نعلم أن الرجوع إلى المبادئ هام جدا وخصوصا أن المشاكل التي تحدث عادة سببها بسيط جدا وأحيانا غير منطقي.

أيمن النعيمي

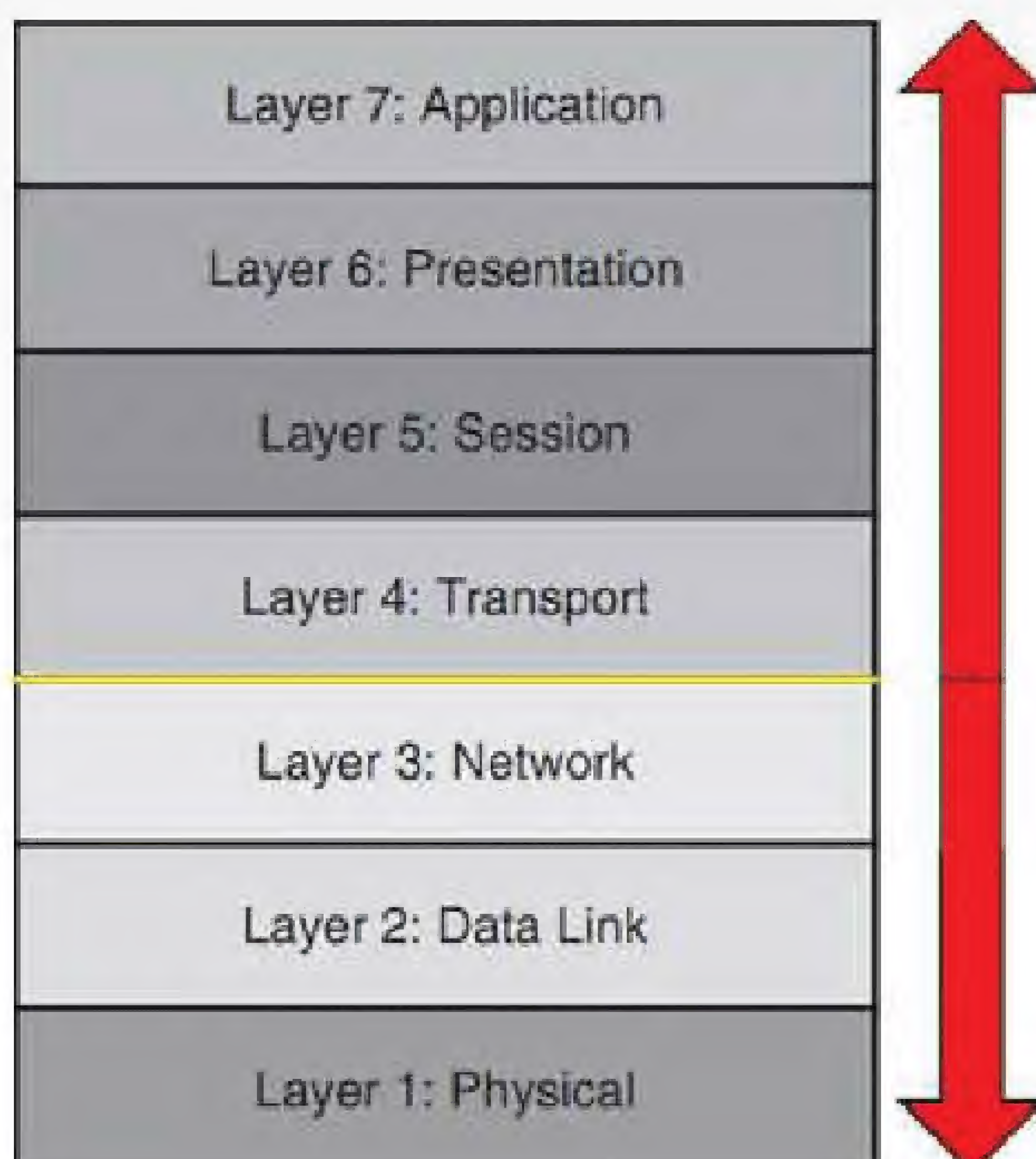
The Bottom-Up Method

نفس فكرة الطريقة الأولى وهي أيضا تعتمد على الـ OSI Layer في حل المشاكل لكن هنا نبدأ من طبقة الـ Physical Layer ونتجه للأعلى وهي طريقة فعالة أيضا لكن غير مناسبة للشركات الكبيرة لأن العمل حينها سوف يأخذ وقتا طويلا، فعلى سبيل المثال لو في حال وجود مشكلة بين عميل وسيرفر سوف يتوجب علينا بداية تفحص الكابلات جميعها الموصولة بين الطرفين وهكذا صعودا إلى طبقات أعلى.



The Divide and Conquer Method

الأسلوب الأكثر شهرة وكفاءة في حل المشاكل، وهو كسابقه يعتمد أيضا على طبقات الـ OSI وهو يبدأ من المنتصف وبعدها يتحدد المكان الذي سوف نتجه إليه، فإما نتجه إلى الـ Transport Layer أو نتجه إلى الـ Network Layer وكمثال بسيط على هذا الأسلوب لنفرض أن أحد الأشخاص لا يمكنه الولوج إلى الـ web Server الموجود في الشركة؟ لو إتبعنا هذا الأسلوب فالحل أن نقوم بعمل Ping إلى السيرفر وننتظر النتائج فلو كانت النتائج إيجابية نتجه إلى الأعلى، ولو سلبية نتجه إلى الأسفل لذلك تعتبر هذه الطريقة أحد أهم وأشهر الطرق لأنها ببساطة توفر الوقت والجهد.



الكابلات

تطورت تقنية الكابلات المستخدمة في نقل البيانات عبر الشبكة حيث كانت اولى التقنيات هي تقنية الكابلات المحورية Coaxial cables ومن ثم دخلت الكابلات المجدولة Twisted Pairs وصولا الى كابلات الالياف الضوئية Fiber Optic والتي احدثت تغير كلي في عالم الكابلات من خلال استعمال الالياف الضوئية الزجاجية والبلاستيكية كمواد تصنيع ومن خلال استعمال الضوء لنقل المعلومات لتدخل ارقاها جديدة لعالم الكابلات من خلال سرعات اكبر ومسافات اطول من النوعين السابقين

أيضا والنهيات المستعملة هي BNC

الكابلات



الكابلات المجدولة

Twisted Pairs

وتعتمد على وجود عدة كابلات مجدولة داخلها تقوم بنقل الإشارة والجدل يتيح امكانية اضعاف تداخل الإشارة فيما بينها وهي عدة انواع ويرمز للنوع بكلمة CAT اختصارا لكلمة CATEGORY

تطورت تقنية الكابلات المستخدمة في نقل البيانات عبر الشبكة حيث كانت اولى التقنيات هي تقنية الكابلات المحورية Coaxial cables ومن ثم دخلت الكابلات المجدولة Twisted Pairs وصولا الى كابلات الالياف الضوئية Fiber Optic والتي احدثت تغير كلي في عالم الكابلات من خلال استعمال الالياف الضوئية الزجاجية والبلاستيكية كمواد تصنيع ومن خلال استعمال الضوء لنقل المعلومات لتدخل ارقاما جديدة لعالم الكابلات من خلال سرعات اكبر ومسافات اطول من النوعين السابقين

Coaxial cables الكابلات المحورية

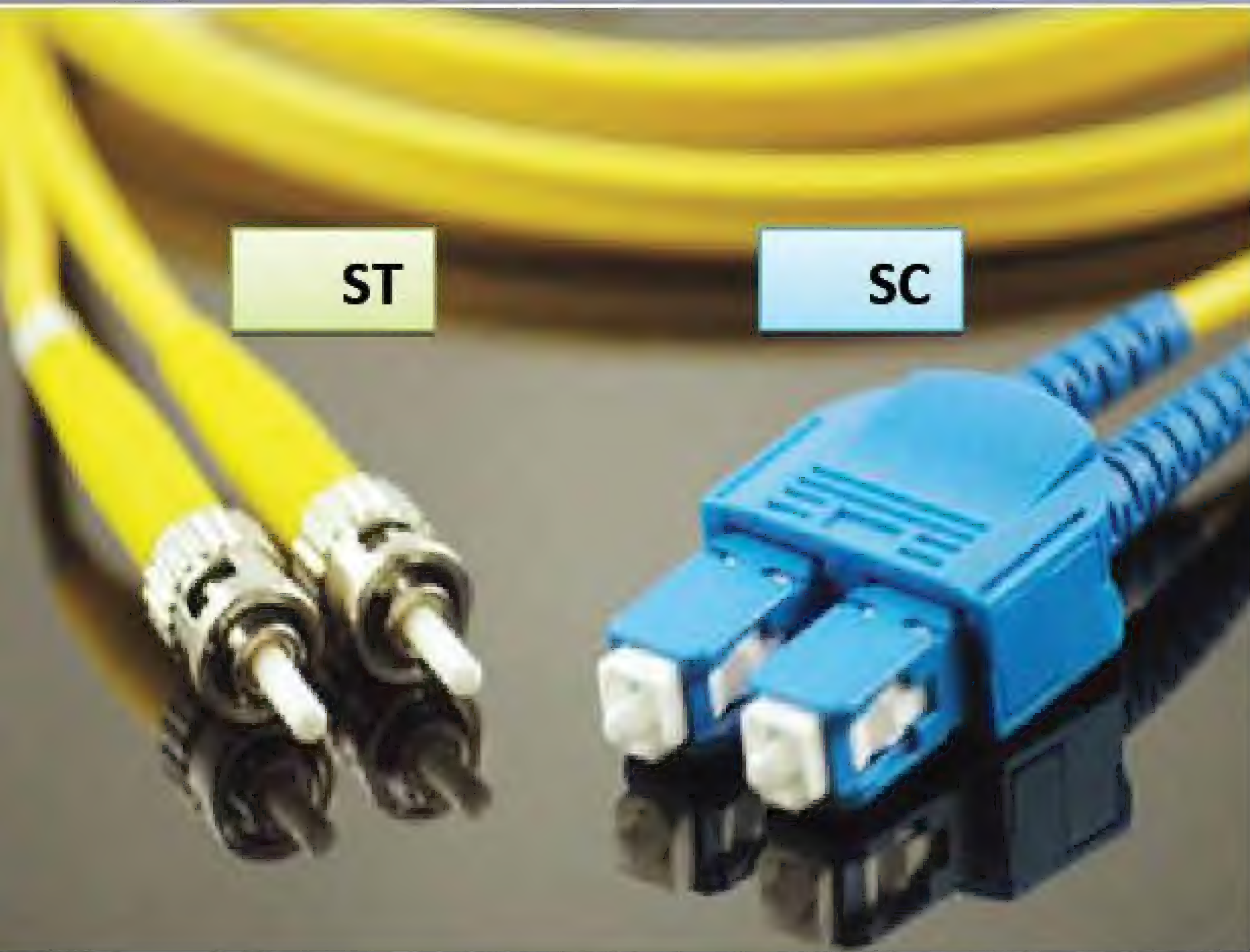
وهو الكابل المستعمل سابقا في نقل اشارات الساتلايت والتلفزيون ويحاط بمادة عازلة وشبكة معدنية وغلاف بلاستيكي



وهي على نوعين رئيسيين كابلات تسمى RG ١٠ Base-U/٥٨ ايضا وهو ينقل البيانات بسرعة ١٠ م بت في الثانية لمسافة قصوى تبلغ ٥٠٠ متر والنوع الاخر ١٠ Base-٢ والتي تنقل البيانات لمسافة ١٨٠ متر وبسرعة ١٠ م بت في الثانية



بالنسبة لحجم البيانات فإنه يمكنك باستخدام هذه التقنيات من نقل كمية من البيانات تتراوح بين ١ الى ١٠ غيغابت في الثانية ولمسافات تتراوح بين ٣٠٠ متر الى مسافات قد تصل في بعض الأنواع الحديثة من هذه التقنية الى ٤٠ كم متر وهذه الأنواع تستعمل في شبكة الانترنت العالمية التي تصل بلدان العالم عبر البر والبحر



تستعمل الاليف البصرية نهايات متعددة واشهرها SC-ST- وتحتاج لتركيبها معدات خاصة لضمان الاستفادة الكبرى من المميزات الخاصة بها وكثيرا مانجد ضياع كبير في السرعة والاداء نتيجة سوء التركيب ان الاليف البصرية كتقنية تعتبر مثلى لنقل البيانات لما فيها من مميزات من حيث السرعة والمسافة ولكن العائق الاهم في وجه انتشارها هو غلاء ثمنها وغلاء المعدات المستعملة بتركيبها.

رضوان سخيطة

ثم صدر الاصدار CAT٥E وهو الاصدار الذي طور من تقنية التصنيع ويقال انه طور من حجم البيانات مع انه صدر رسميا بسرعة ١٠٠ م بت في الثانية ومن ثم تبعه الاصدار التالي CAT٦ وهو الذي دخل معه عالم الكابلات عالم ال Giga ethernet اي سرعة الألفم بت في الثانية

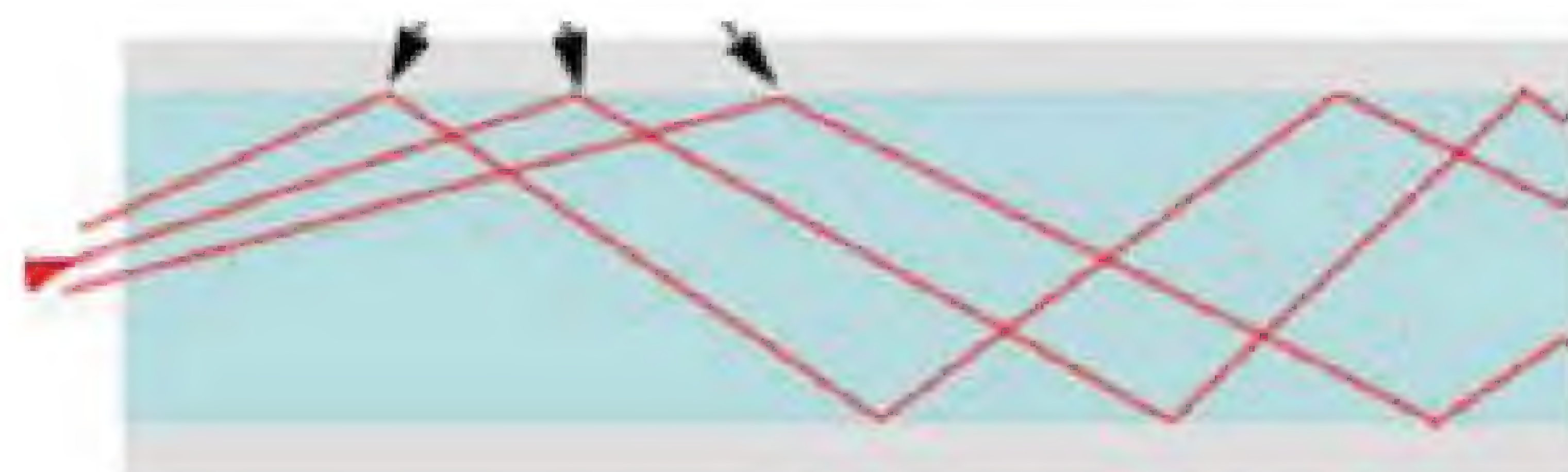
تشارك كل الفئات في كون المدى الاقصى لها هو ١٠٠ متر وكونها تستعمل RG٤٥ كنهايات لها

كابلات الألياف البصرية (الضوئية) Fiber Optic

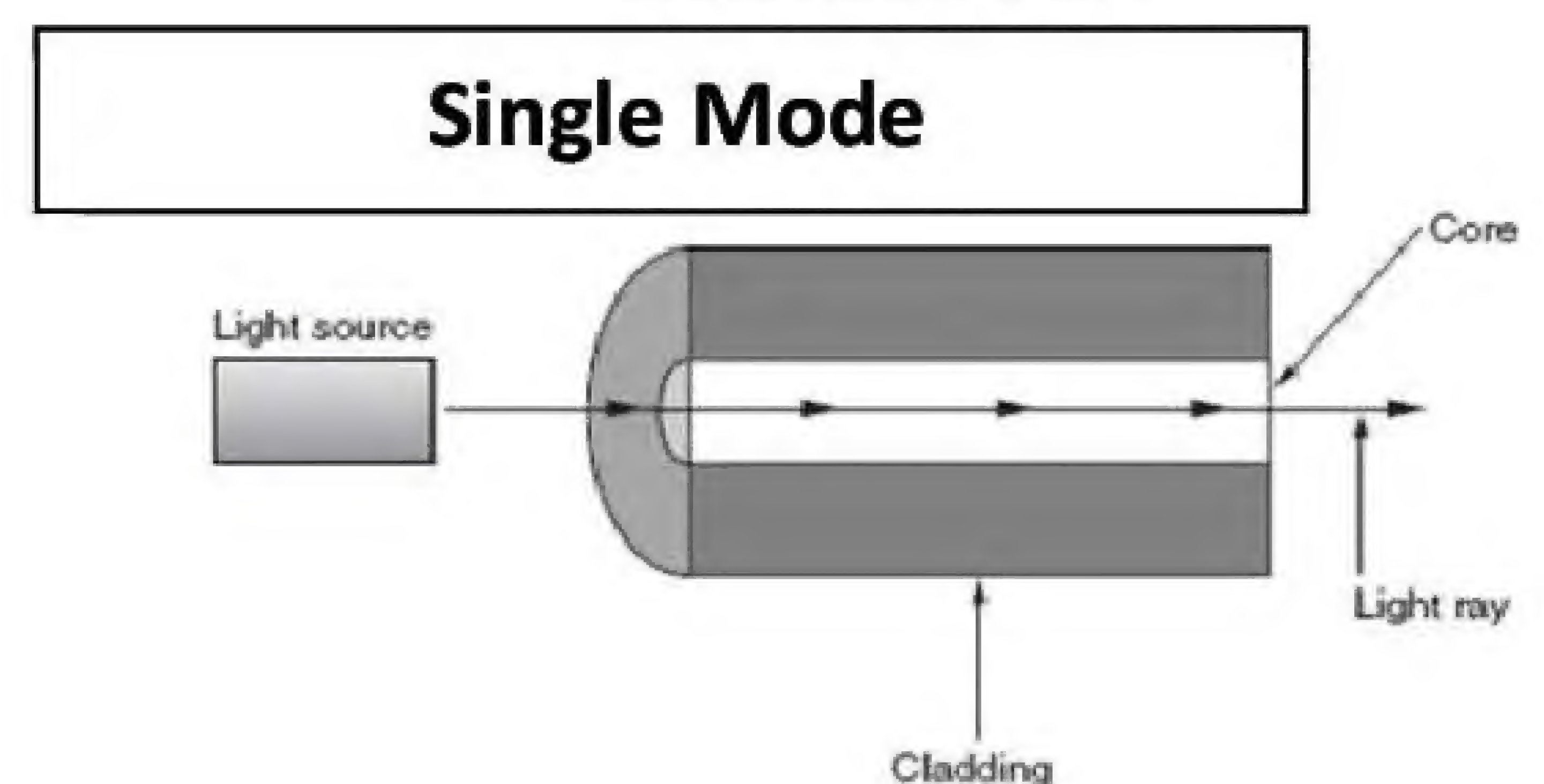
وهي أحدث التقنيات في نقل البيانات بسرعات كبيرة ولمسافات كبيرة جدا حيث بالامكان نقل البيانات عبر المدن باستخدام هذه التقنيات ومن اهم المميزات عن التقنيات السابقة هو كونها لا تتأثر بالتداخل الكهرومغناطيسي (RFI-EMI) كون الناقل فيها هو الضوء وليس الاشارات الكهربائية ، وتقسم من حيث الانواع الى اليف بلاستيكية واليف زجاجية وكتقنيات نقل فانها تقسم الى اليف وحيدة النمط single mode ومتعددة النمط Multi Mode



وعامة تستعمل الاليف الضوئية احادية النمط في نقل البيانات لمسافات طويلة في حين ان الاليف الضوئية متعددة النمط تنقل حجم اكبر من البيانات ولمسافات اقل



Multimode Fiber



Data Link Flow Control Protocols

سوف اتحدث اليوم في اول مقال لي عن البروتوكولات المسئولة عن كيفية حدوث ال flow control والتأكد من ان جميع ال frames وصلت سليمة الى receiver وماهى المشاكل التى قد تحدث اثناء ارسالها.

سوف اختص الان بتوضيح بروتوكول ال Automatic Repeat reQuest (ARQ) Protocols
يوجد ثلاثه انواع من هذا البروتوكول وهي على الشكل الآتي:

Stop-and-wait ARQ-1

Go-Back-N ARQ-۲

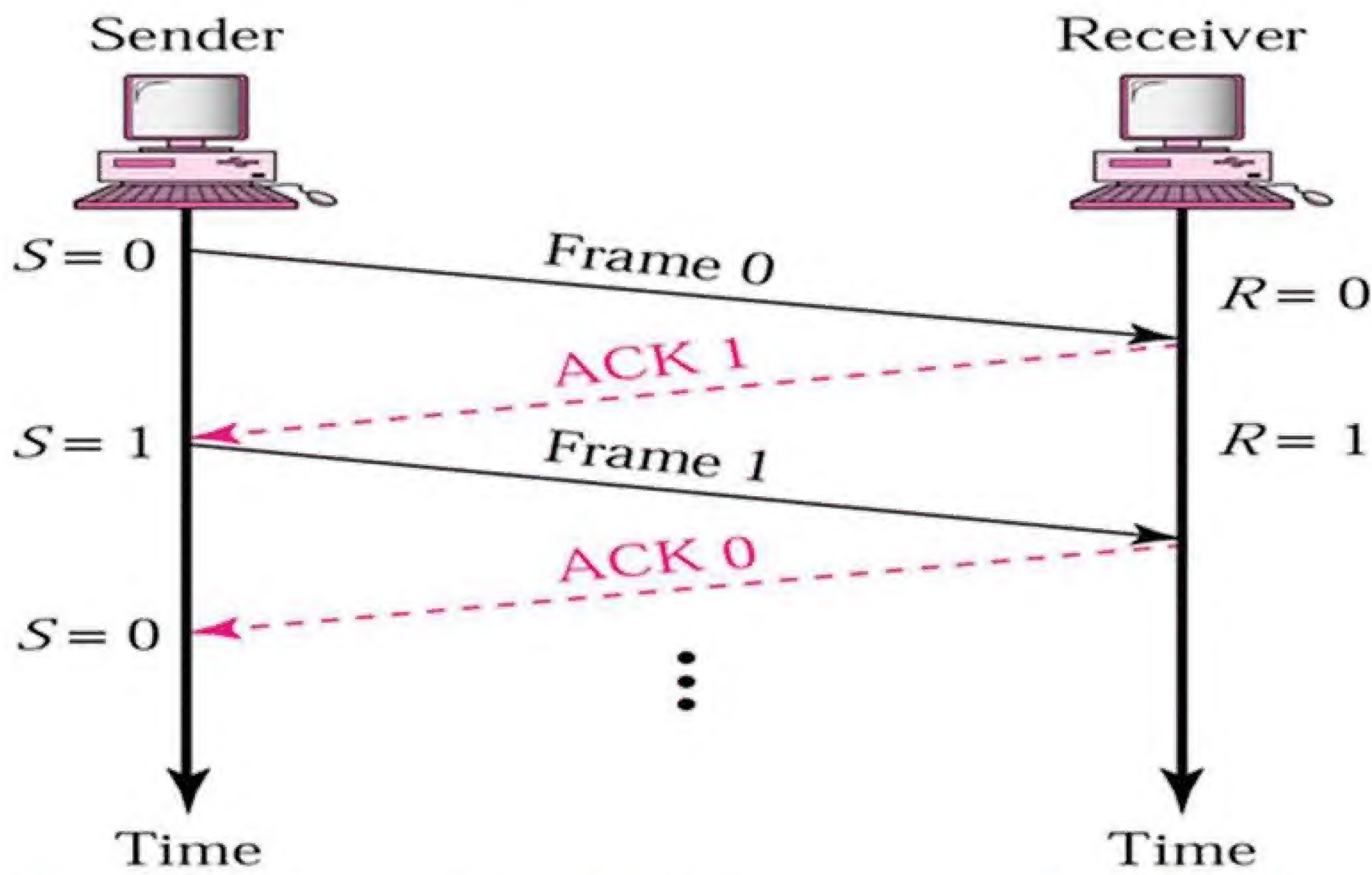
Selective Repeat ARQ-۳

وطبعا جميع هذه البروتوكولات تعمل ف ال Data Link وال Transport Layers فى ال OSI model

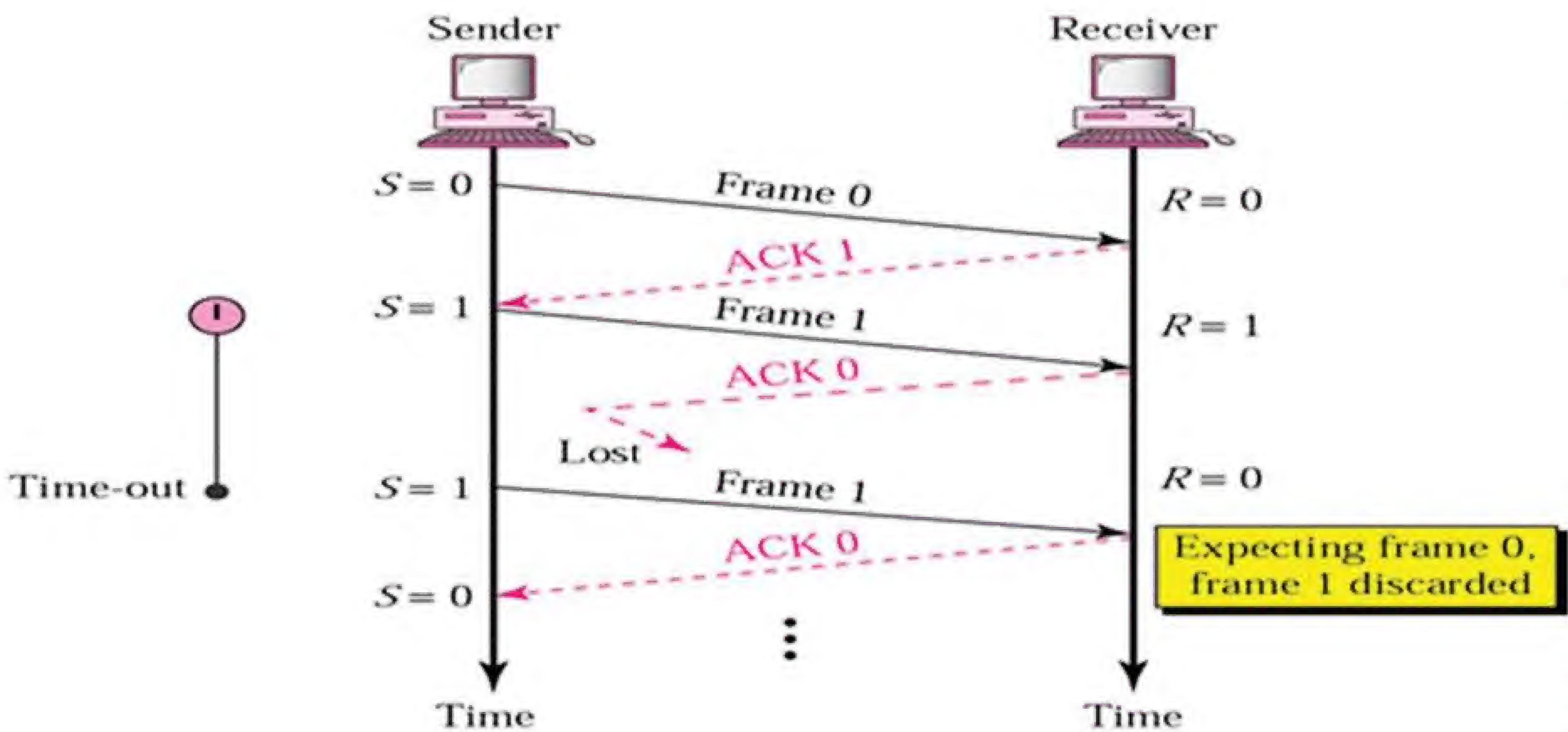
Stop-and-wait ARQ: اولاً

طريقه عمل هذا البروتوكول ان ال sender يرسل فريم واحد فقط الى ال receiver و عندما يستقبله ال receiver ويتأكد انه كامل و سليم يرسل ack الى ال sender فيرسل فريم اخر وهكذا.

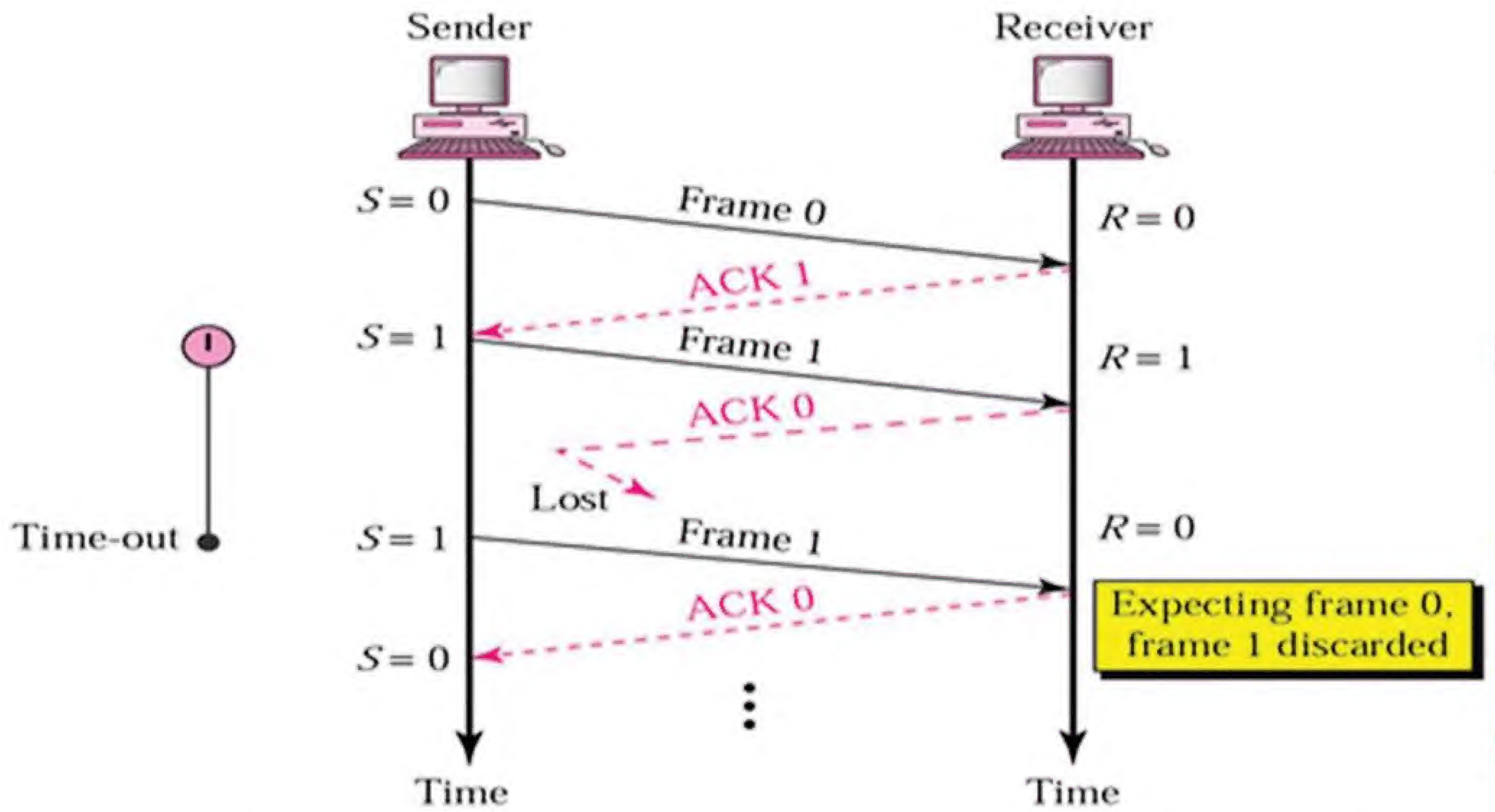
وهناك مشكلتين في هذا البروتوكول وهما



١- في حالة عدم وصول الفريم الى ال receiver «يعنى الفريم وقع في الطريق»



وحلها هو ان ال sender عندما يرسل الفريم يبدأ ف تشغيل timer واذا لم تصل ال ack قبل انتهاء ال timer يرسل الفريم مره اخره ودا طبعا عيب في هذا البروتوكول لان ال channel بتفضل فاضيه طول فتره ارسال الفريم وانتظار ال ack مما يودي الى فقدان جزء كبير من ال bandwidth
٢- في حاله عدم وصول ack الى ال sender «يعنى ack وقعت في الطريق»



هينتظر الى ان ينهى ال timer وبعدها يبدأ ال sender في ارسال الفريم مره اخرى وعندما يصل الى receiver هيعمله discard لانه اصل وصلوا مره قبل كده ونلاحظ هنا ايضا نفس العيب الموجود ف الحاله الاولى

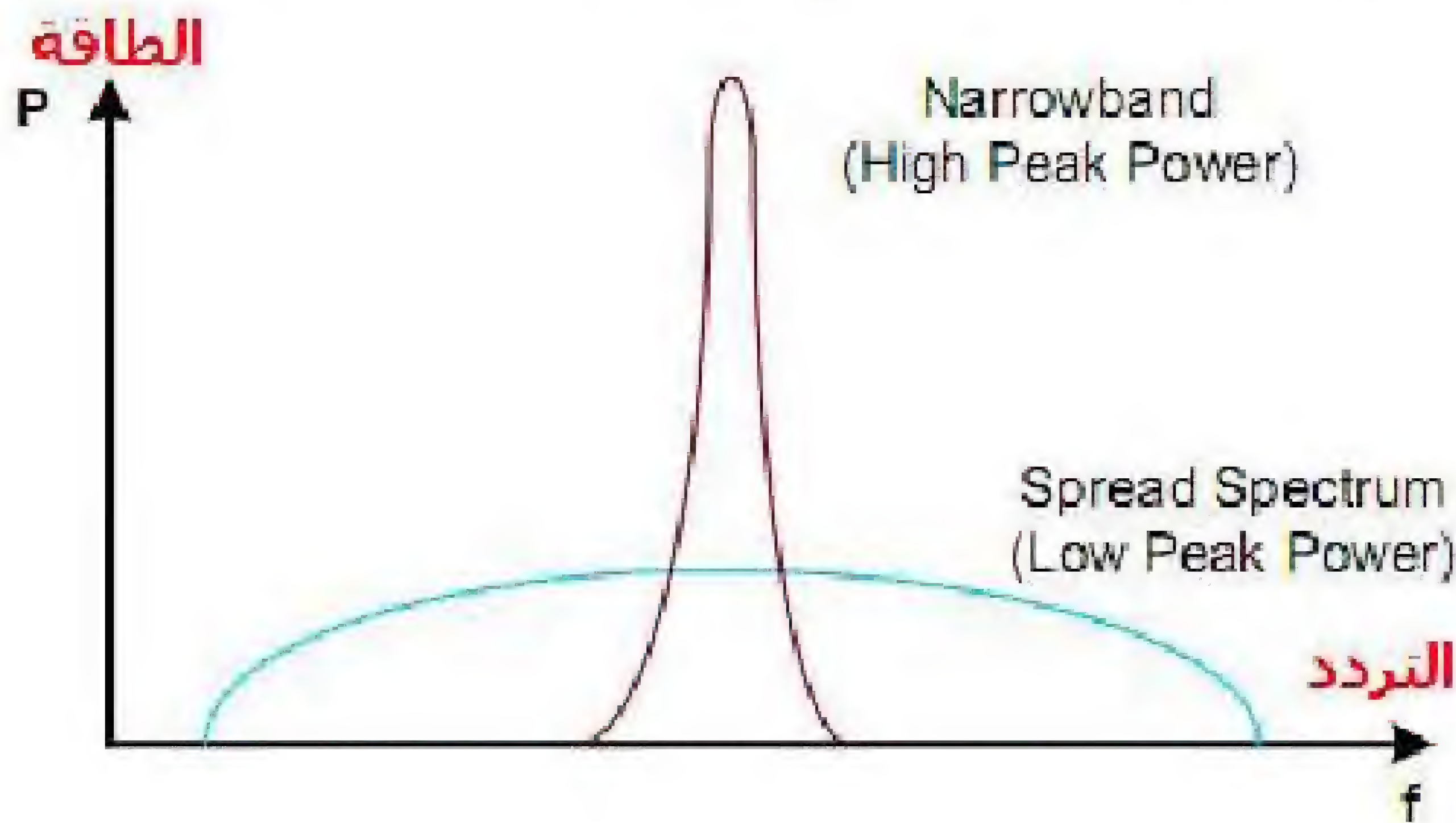
أنتظرونا في العدد القادم لنكمل باقي المقال

مصطفى حسن

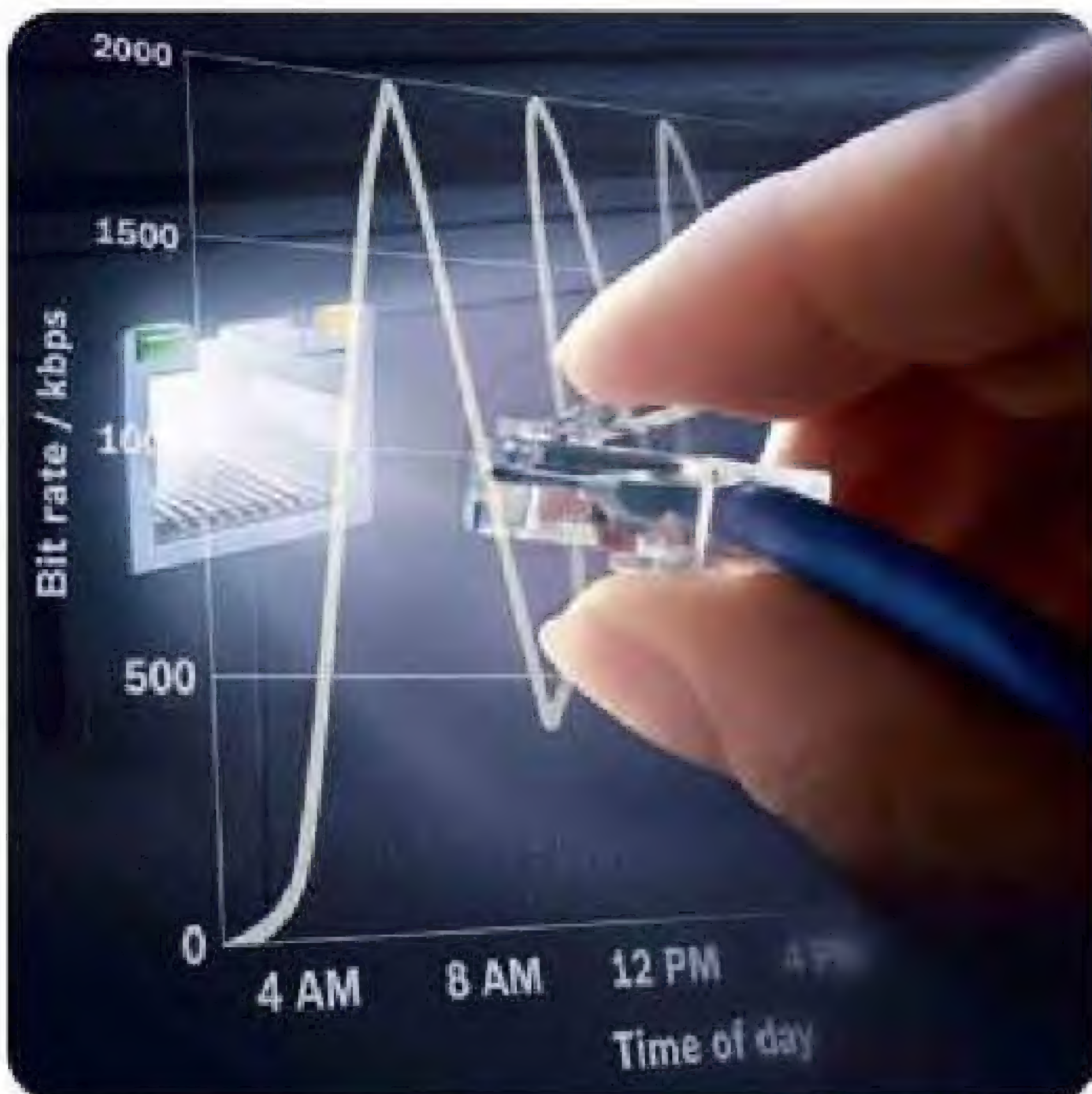
بداية الشبكات اللاسلكية



كانت حزمة الترددات عريضة يزداد معدل نقل البيانات.



و يستخدم الطيف المنتشر في الهواتف اللاسلكية وفي نظام الملاحة GPS وفي الشبكات اللاسلكية المختلفة حيث يتم تمديد الطيف لكي يغطي كامل عرض الحزمة المتاح مع تمكينها في الوقت ذاته لعدد من المستخدمين في التشارك. المدى الترددي Bandwidth



علي الرغم من أن الشبكات اللاسلكية لم تعرف إلا بعد عام ١٩٩٠، إلا أن عالم الاتصالات اللاسلكية كان أقدم بكثير من هذا التاريخ، فقد بدأ بزوغ نجم هذا العلم علي يد فلكي بريطاني اسمه ويليام هرتشل William Herschel (١٧٣٨ - ١٨٢٢)، و ذلك عندما إكتشف أن هناك طيف أو أشعة غير مرئية للعين المجردة مجاور لأسفل الطيف المرئي و قد سمي هذا الطيف بالأشعة تحت الحمراء - لأنها ظهرت تحت طيف الأشعة الحمراء - و قد قاد هذا الإكتشاف إلى ظهور نظرية الأمواج الكهرومغناطيسية wave Theory Electromagnetic، و التي تم دراستها و تطويرها بإستفاضة من قبل العالم الفيزيائي جيمس ماكسويل James Maxwell (١٨٣١ - ١٨٧٩) ثم بواسطة العالم مايكل فاراداي Michael Faraday (١٧٩١ - ١٨٦٧) الذي إستطاع أن يثبت اقدم هذا العلم و من قبلهم أندريه ماري أمبير Andre-Marie Ampere (١٧٧٥ - ١٨٣٦)، ثم جاء الإكتشاف الأكبر للعالم هاينريش هيرتز Heinrich Hertz (١٨٥٧ - ١٨٩٤) الذي أثبت أن الموجات الكهرومغناطيسية تستطيع السير بسرعة تساوي سرعة الضوء و تستطيع أيضا أن تنقل الإشارات الكهربائية.

و في حالة إذا إستطعنا تطوير هذه النظرية على أرض الواقع فإننا نستطيع أن ننقل أي إشارة كهربائية عبر الهواء و لكن تجابهنا عدة تحديات أهمها هو إمكانية نقل الإشارة لمسافات بنفس إمكانية الكابلات بل و حماية الإشارة أثناء نقلها، وهما التحديان اللذان وجدا مع شبكات ال LAN عند تحويلها إلى شبكات لاسلكية WLAN.

و لقد كانت هناك تحديات في إستخدام الإتصال اللاسلكي كوسيلة للنقل في الشبكة و من أهم تلك التحديات هو أسلوب النقل و المدى الترددي Bandwidth و تقنيات التعديل Modulation هذه التحديات أسلوب نقل الإشارة اللاسلكية يتم نقل أي إشارة لاسلكية بطريقتين:

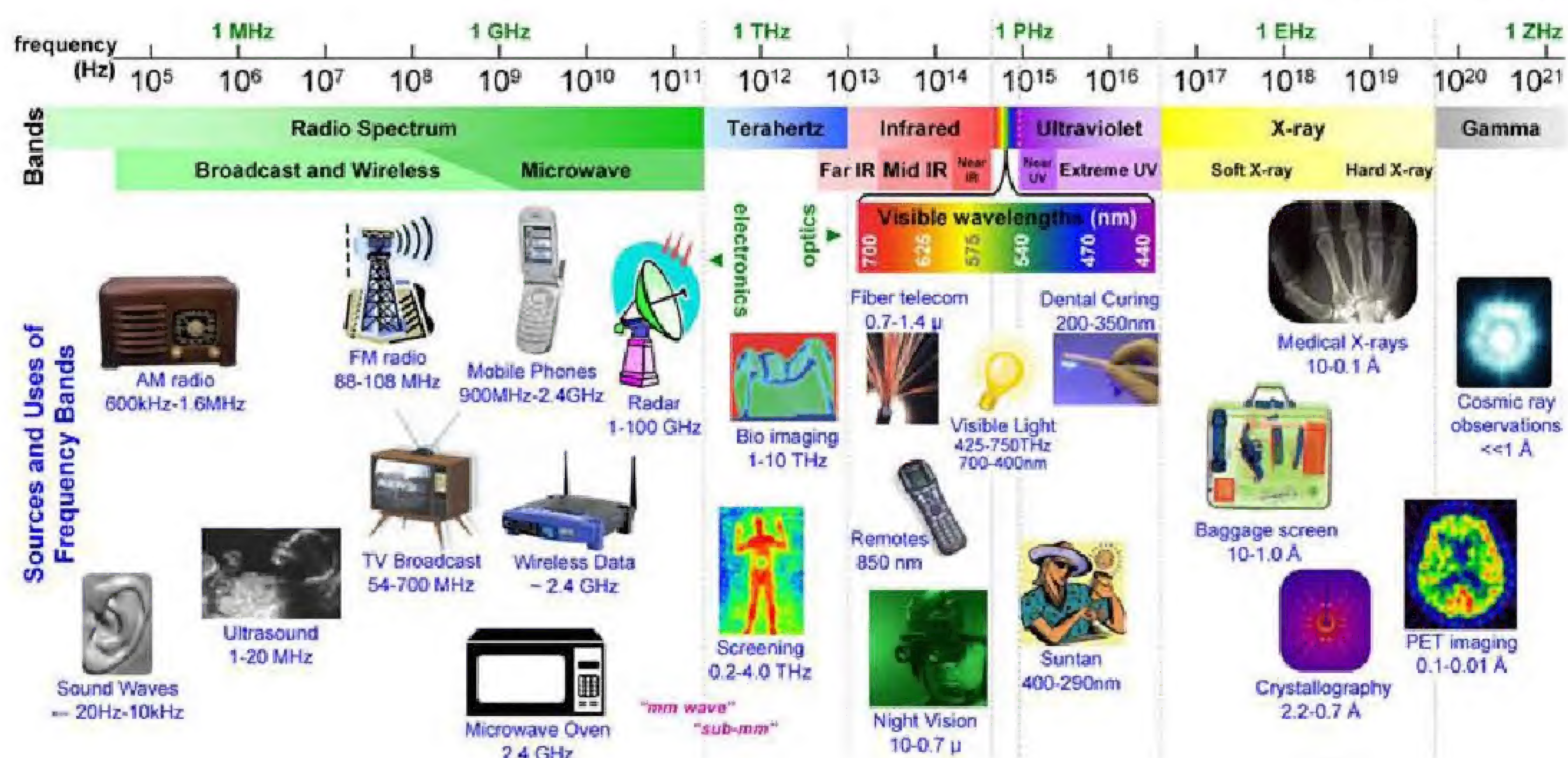
أولا بواسطة نطاق ضيق ذو تردد أحادي يطلق عليه اسم Narrow Band و يستخدم طاقة إرسال عالية. ثانيا بواسطة نطاق واسع ذو مجموعة ترددات يطلق عليه اسم Spread Spectrum و يستخدم طاقة إرسال منخفضة، و قد تم إعتداد النطاق الواسع أو المنتشر Spread Spectrum لأنه يستخدم قوة إرسال خفيفة وحزمة عريضة من الترددات، و من المعروف أنه كلما

في عالم اللاسلكي يطلق مصطلح المدى الترددي على شيئين أولهما عرض القناة RF Channel التي ترسل فيها الإشارة و ثانيهما هو Data Rate أى معدل نقل البيانات و يتم تمييزها بالهرتز Hz و هي وحدة التردد و هو دورة واحدة في الثانية و من المعروف أن الطيف الكهرومغناطيسي للترددات تم تقسيمه الى نطاقات كل منها يخص تطبيقات معينة منها نطاقات تحتاج تراخيص للتعامل معها و أخرى متروكة للتعامل معها بحرية.

و في الشكل التالي يوجد مخطط كامل للنطاقات الترددية مع التطبيقات المستخدمة فيها، و يبدأ النطاق المستخدم مع ترددات الصوت المسموعة ثم يعلو إلى الموجات فوق الصوتية المستخدمة في أجهزة السونار الطبية ثم ترددات AM و FM و هي نطاقات مرخصة للتعامل مع أجهزة المذياع و التلفاز و يطلق عليها موجات الراديو ثم يعلو الطيف إلى موجات الميكروويف المستخدمة في شبكات الموبايل و أجهزة الرادار و أجهزة الميكروويف المنزلي ثم يأتي نطاق وسيط يفصل بين الطيف الإلكتروني و هو هذا الذي تكلمنا عنه و الطيف المرئي و هو الضوء العادي الذي نراه بألوانه السبعة الذي يبدأ من بعد الأشعة تحت الحمراء و ينتهي قبل الأشعة فوق البنفسجية ثم يدخل الطيف إلى الترددات العالية جدا و ذلك مع الموجات السينية X ray ثم الموجات الذرية و الكونية، و علي هذا فإن الطيف الكهرومغناطيسي يبدأ من ELF – Extremely Low frequency ٣٠HZ-٣ و حتى EHF – Extremely High Frequency ٣٠GHZ-٣٠٠GHZ حيث يتم تقسيم هذا الطيف طبقا للتردد من الأدنى إلى الأعلى هكذا

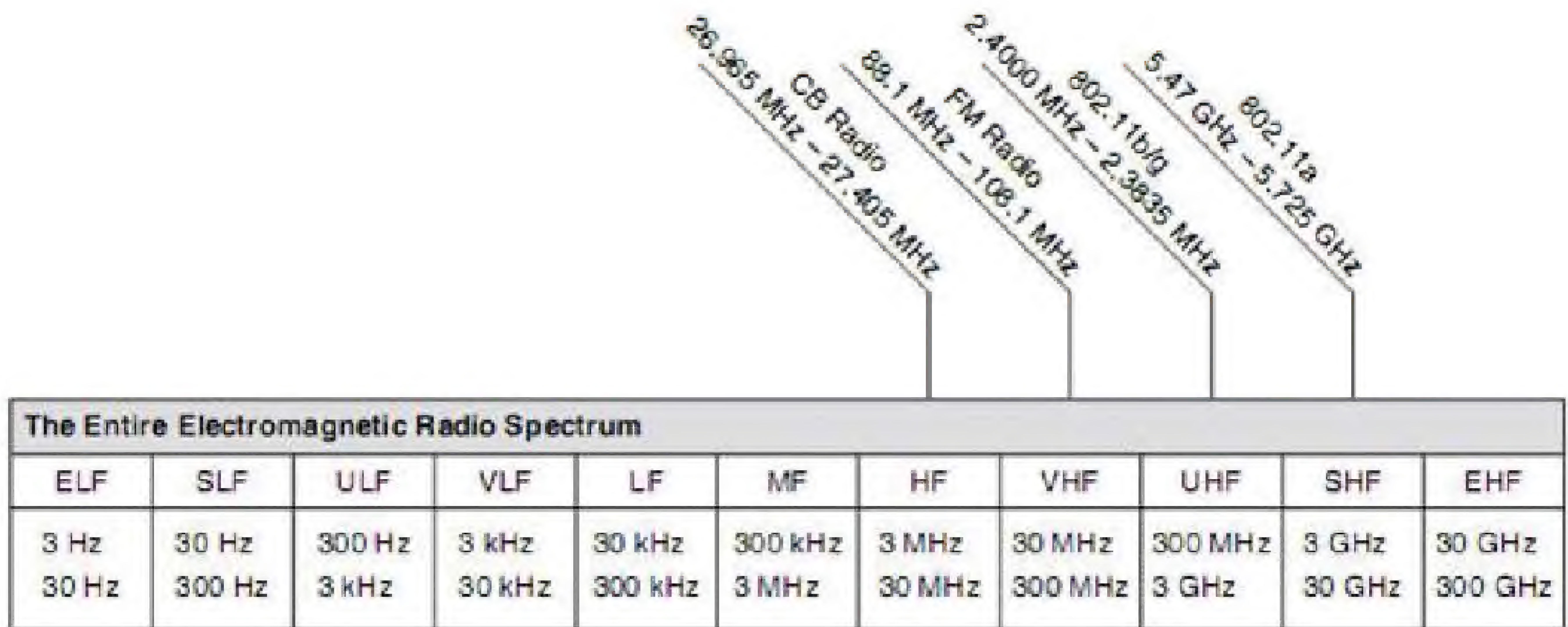
LF- HF- UHF- SHF-EHF-IF

و عند بدء التعامل مع الشبكات اللاسلكية كان التفكير في استخدام نطاق ترددي غير تجارى هو البديهي لإمكانية التعامل به علي نطاق واسع بدون الحاجة إلى تراخيص حكومية لحجز التردد، و يوجد في هذا الطيف الكهرومغناطيسي مناطق للإستخدام غير التجارى مثل نطاق Citizen Band ZB و هو نطاق ترددي يستخدمه هواة اللاسلكي على مستوى العالم و هو لا يصلح هنا لأن نطاقه ضيق جدا حيث لا يتعدى مداه الترددي عن ٣ khz و لذلك تم اللجوء إلى نطاق أعلى يطلق عليه ISM Band حيث ISM هي الحروف الأولى من الكلمات industrial، scientific and medical و يستخدم هذا النطاق في الأجهزة الطبية و المنزلية و الصناعية التي تتعامل مع ترددات عالية مثل أجهزة الميكروويف المنزلية و بعض أجهزة الأشعة الطبية و الصناعية، غير أن وجود هذه الأجهزة في حيز الشبكة اللاسلكية يؤدي لحدوث تضارب و تداخل بين هذه الترددات.



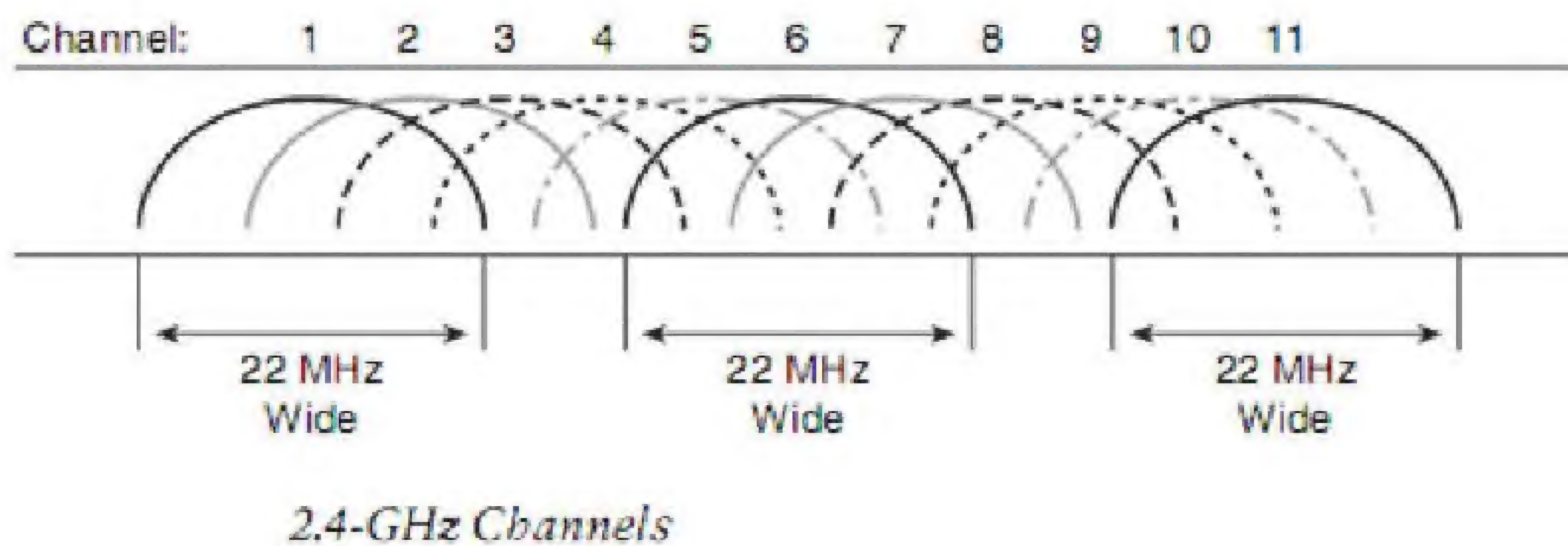
و قد تم إختيار ثلاث ترددات لهذا الأمر هي ٩٠٠ MHz، ٢.٤ GHz، و ٩٠٠ GHz و على هذا فإن شبكتنا اللاسلكية و أجهزتها توجد في نطاق SHF و UHF ٩٠٠ MHz

هذا النطاق يبدأ من ٩٠٢ ميغا هرتز و حتى ٩٢٨ ميغا هرتز و هو نفس مدى أجهزة الهواتف اللاسلكية و يعمل بنفس الطريقة حيث تقوم بإختيار القناة التي تحب أن تعمل عليها و لا تكون



٢,٤ GHZ

يعتبر هذا المدى الأكثر إستخداما في عالم الشبكات اللاسلكية حيث يستخدم من قبل معايير IEEE ٨٠٢,١ و IEEE ٨٠٢,١١b إلى ١١ قناة عرض كل قناة ٢٢ ميغا هرتز و بالطبع ستجد تداخل بين هذه القنوات مما يمنع إستخدام القنوات المتجاورة لنفس الشبكة اللاسلكية بل يتم إستخدام القنوات رقم ١ و ٦ و ١١ و لهذا فلا تستغرب أن يقوم بعض المصنعون بإجبارك على الإختيار بين هذه الثلاث قنوات فقط في أجهزتهم.



و يكون معدل نقل البيانات في هذا النطاق ما بين ١ و ٢ و ٥,٥ و ١١ ميجا بت لكل ثانية و يستخدم هذا النطاق الترددي تقنية تعديل إرسال تسمى DSSS Direct Sequence Spread Spectrum Modulation ٥GHZ

يستخدم هذا النطاق مع ٨٠٢,١١a و ٨٠٢,١١n و يكون معدل نقل البيانات ما بين ٦ ميجا بت لكل ثانية و ٩ و ١٢ و ١٨ و ٢٤ و ٣٦ و ٤٨ و حتى ٥٤ ميجا بت لكل ثانية. و لا يعتبر هذا النطاق بنفس شهرة النطاق السابق و ذلك لأن المصنعون قد إبتعدوا عن تصنيع أجهزة تدعم فقط ٨٠٢,١١a منذ ٢٠٠١ إلا أن وجود ٨٠٢,١١n قد أنعش سوق هذا النطاق مرة أخرى. و كسابقه يتم تقسيمه إلى عدة قنوات ترددية و يبلغ عددها ٢٣ قناة متداخلة بعرض ٢٠ ميغا هرتز لكل قناة يستخدم هذا النطاق تقنية تعديل إرسال تسمى OFDM Orthogonal Frequency Division Multiplexing .

Cryptography Part II

Classical Encryption

ما هي الطرق الكلاسيكية في التشفير Classical Method :-

هي طرق قديمة استخدمت في فترات الحرب خاصة الحرب العالمية الأولى و الثانية، حيث كانت الرسائل تكتب

باليد، و كان الخوف هو أن تقع هذه الرسائل في يد العدو، لذلك كانوا يقومون بعملية تبديل لأماكن الأحرف Transposition، أو تبديل الحرف بحرف آخر Substitution، وذلك حسب قواعد معينة أو خوارزمية تتحكم في هذه العملية، و في وقتنا الحالي لم يعد هناك أى استخدام لهذه الطرق، فلا يوجد فائدة من استخدام هذه الطرق القديمة (Classical Method)، لأنها سهلة الكسر و سنعرف هذا لاحقا بل هناك طرق تشفير حديثة (Modern Cryptography) يتم استخدامها الآن في مختلف المجالات، أما من يقول لى لماذا أتحدث عنها الآن؟ فإنى أتحدث عن هذه الطرق للأسباب الآتية:-

١- كون هذه هي الطرق التى نشأ منها هذا العلم فيجب أن تبدأ بها حتى تفهم الفكرة العامة و المصطلحات.

٢- هي تنمى العقل بشدة و من الممكن أن تجد نفسك موهوب في هذا المجال و تجد متعة كبيرة فيه، و من الممكن أن تجد الامر صعبا معقدا، بإختصار ستجد إجابة سؤال «هل أصلح لهذا المجال؟» عندما تحاول تعلم هذه الطرق، من يعلم ربما تكون عبقرى.

٣- هي أساس العديد من الطرق الحديثة.

ألا ترى معى الآن أنه من المفيد أن نلقى نظرة على هذه الطرق ؟

سينقسم المقال إلى جزئين، الجزء الأول هو جزء نظرى نتعرف فيه على المصطلحات المهمة، و الجزء الآخر سنأخذ بعض الأمثلة لتعميق الفهم.

الجزء النظرى :-

يوجد الكثير و الكثير من المصطلحات و لكن سأكتب أهمها الآن و التى سنستخدمها بكثرة.

- Plaintext: هذا هو النص الأصلي المراد إخفائه من العملية كلها، و هذا النص هو ما سيتم إدخاله في خوارزمية التشفير كـ Input .

- Encryption algorithm: هذا هو الجزء المهم من العملية الذى يحدد القواعد التى سنتبعها في عملية التشفير، فخوارزميات التشفير يمكن تخيلها كبوابه يدخل منها شخص و يخرج منها بشكل مختلف.

- Secret key: هذا هو الجزء الخطير في الأمر و هو مفتاح التشفير، و هو أيضا من مدخلات

خوارزمية التشفير، أى أننا نقوم بإدخال شيئين في ال Encryption algorithm و هما النص

الأصلى المراد تشفيره، و ندخل معه مفتاح التشفير. نرجع إلى مثال البوابة السابق و التى هي عبارة

عن خوارزمية تشفير يمر من خلالها شخص و الذى هو عبارة عن ال Plain Text الذى نحتاج إلى

أن نشفره و معه مفتاح التشفير الذى سيؤثر على شكل ال plain text بعد التشفير، مثلا إذا أردنا

أن نشفر حرف P التى تدل على Plain Text بإستخدام الخوارزمية E التى تدل على عملية ال

Encryption بإستخدام المفتاح K-1 نفترض أن يكون النص المشفر X على سبيل المثال ، فإذا قمنا

بتطبيق هذه العملية مرة أخرى و قمنا بتغيير المفتاح فقط لا غير بمفتاح آخر، لنفترض K-2 سيكون

النتائج مختلف تماما على سبيل المثال Y، بهذا نستنتج الآتى فمفتاح التشفير Encryption Key سيؤثر

على مخرجات عملية التشفير.

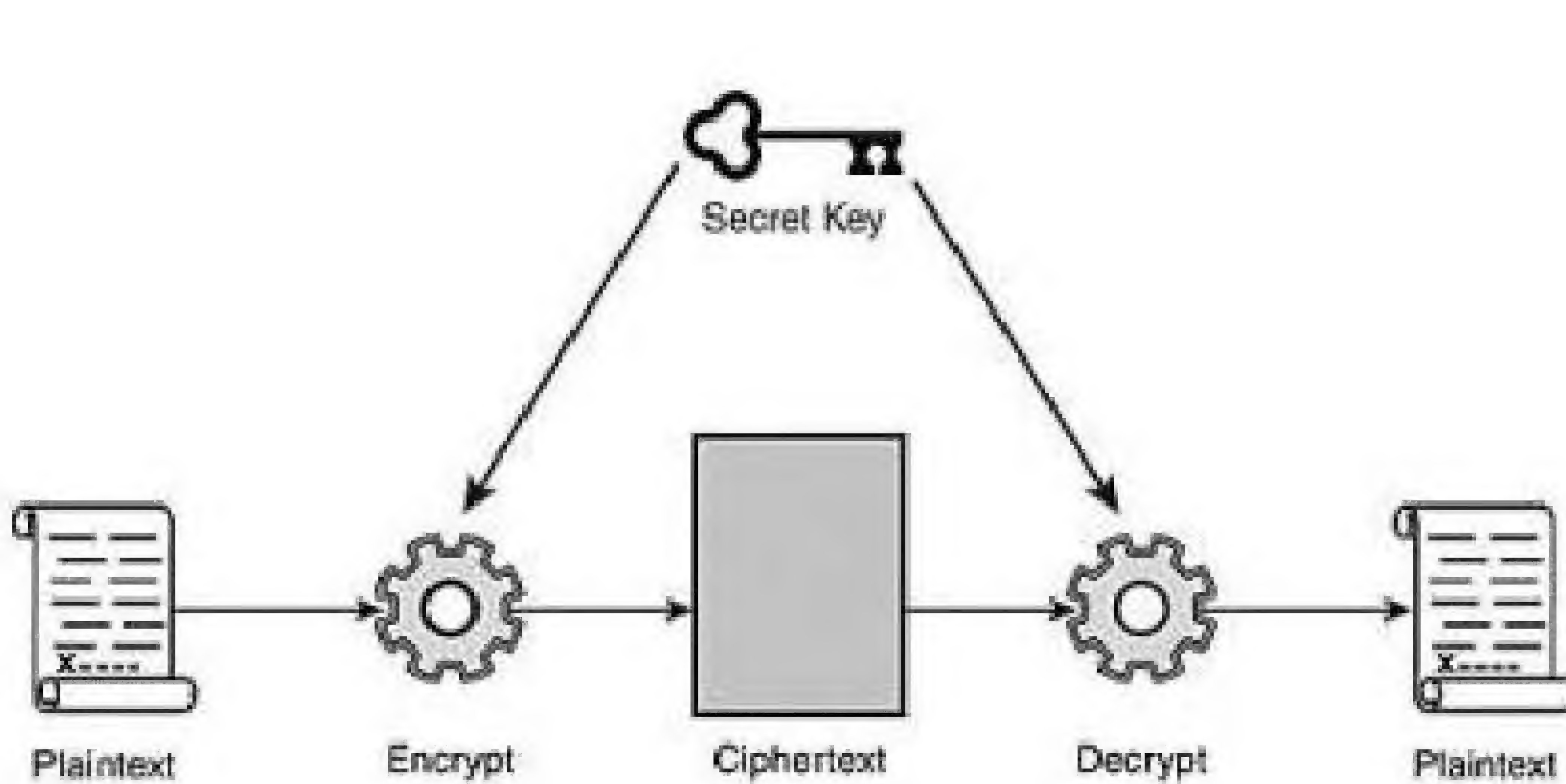
- **Ciphertext**: هذا هو الشخص الجديد الذي سيخرج من البوابة، لو رجعنا إلى مثالنا السابق، أى أنه عبارة عن كلام غير مفهوم و مشفر و نستطيع أن ننقل هذا النص المشفر بدون قلق لأنه لو وقع فى يد شخص لن يفهم منه شيء أبدا.

- **Decryption algorithm**: هذه هي القطعة الأخيرة فى العملية، مثلا بعد أن قمنا بتشفير ال Plain Text و قمنا بإرساله إلى الطرف الآخر بأمان، الآن كيف يقرأ الطرف الآخر هذه الرسالة ؟ فى الحقيقة الطرف الآخر يجب أن يكون عنده خوارزمية أخرى تسمى **Decryption algorithm**، و هي نفس ال **Encryption Algorithm** و لكن بالعكس، يقوم الطرف الآخر بإدخال النص المشفر و نفس مفتاح التشفير الذى تم استخدامه فى عملية التشفير ك INPUT لل **Decryption algorithm** ليعود النص كما كان، أى أن مفتاح التشفير هو أهم شيء فى العملية كلها، و إذا عرفه شخص ثالث و وقع بين يديه النص المشفر و بالطبع يعلم ال **Encryption algorithm** ليقوم بعكسها فسيستطيع هذا الشخص فك التشفير، و لأن خوارزمية التشفير لا تعتبر سرا، بل إنه يمكن يمكن معرفتها، فعندئذ الجزء الذى يجب أن نحافظ على سرية هو مفتاح التشفير.

- **cryptographer**: هذا هو الشخص الذى يقوم ببناء خوارزميات التشفير و تطويرها و سنتعرف على أحدهم فى آخر المقال .

- **cryptanalyst**: يقوم هذا الشخص بمحاولة كشف نقاط الضعف فى الخوارزميات و هي بمثابة خدمة لل **cryptographer** لأنه يعرفه ثغرات الخوارزمية، و بالتالى يقوم بتطويرها، مثل المبرمج و الهكر الثانى يقوم بإيجاد ثغرات لنظام الأول و من ثم يقوم الأول بترقيعها و هكذا. يوجد عند معظم الجيوش و الأجهزة الإستخباراتية فريق من العلماء يقومون بهذا الدور.

- **Cryptanalysis**: هو الفرع الذى يختص بمحاولة تحليل الخوارزميات و معرفه طريقة عملها.



الجزء العملى :-

هذا هو الجزء العملى الذى سنفهم به أكثر الكلام السابق عندما نقوم بتطبيقه. تنقسم الطرق الكلاسيكية أو القديمة إلى نوعين، النوع الأول يسمى **Substitution Cipher** أى تبديل الحرف بحرف آخر، النوع الثانى يسمى **Transposition** أى تغيير مكان الحرف فقط و عدم تغيير الحرف نفسه، و لنبدأ بالنوع الأول.

شفرات الإحلال - **Substitution Cipher**

تنقسم شفرات الإحلال **Substitution Cipher** إلى أربعة أنواع مختلفة كالآتى :-

- النوع الأول : **Monoalphabetic Substitution Cipher**
- النوع الثانى : **Polyalphabetic Substitution Cipher**
- النوع الثالث : **Polygram Substitution Cipher**
- النوع الرابع : **Homophonic Substitution Cipher**

ركزوا معى فقط فى النوع الأول حتى لا تزيد الأمور تعقيدا

شفرات **Monoalphabetic Substitution Cipher** :

من أقدم الطرق التى إستخدمت فى التشفير. فكرتها الأساسية تتلخص فى تغيير حرف إلى حرف آخر، يندرج تحت هذا النوع العديد من الشفرات أو خوارزميات التشفير أشهرهم:

- **Affine Cipher**

- Caesar Cipher
- Cipher ROT13
- Abash Cipher

هذه هي طرق التشفير نفسها، أتمنى أن يفهم القارئ هذه النقطة جيدا.

نبدأ بشفرة أو خوارزمية قيصر Caesar Cipher :

هي من أبسط الشفرات و أسهلها في الكسر. نفترض أننا نريد تشفير هذه الجملة «Encipher Me» و مفتاح التشفير هو رقم ٣ سنفهم معنى هذا حالا و طبعا خوارزمية التشفير هي شفرة قيصر، لنلخص المعطيات كالآتي:

PlainText Letters : A B C D E F X Y Z
CipherText Lettes : D E F G H I A B C
NETWORKSET

Plain Text = «Encipher Me»

Encryption Algorithm = «Caesar Cipher»

KEY = ٣

Cipher Text = ??

الآن يجب أن نحسب النص المشفر و لعمل ذلك من خلال شفرة قيصر سنقوم بعدة خطوات، أولها هو ترتيب الحروف الإنجليزية من A إلى Z في جدول و ترقيم هذه الأحرف، يعني A سيكون رقمه ٠ و B رقمه ١ و C رقمة ٢ إلى آخره

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

..... حتى يتكون لدينا الجدول التالي:

الآن نستطيع أن نبدأ تشفير الجملة «Encipher Me»، لنبدأ بالحرف الأول في الجملة E و ننظر إلى الرقم المقابل له بالجدول و هو ٤، نقوم بجمع قيمة المفتاح مع هذا الرقم كالآتي $4+3=7$ ، لاحظ إستخدام قيمة المفتاح ٣. الآن ننظر إلى الجدول مرة أخرى و نبحث عن الحرف المقابل للرقم الناتج الذي هو ٧ و الحرف المقابل هو H، هكذا قمنا بتبديل الحرف E إلى H، و هكذا مع باقى الأحرف حيث سيكون التشفير كالتالي:

E=h - N=q - C=f - I=L - P=s - H=k - E=h - R=u - M=P - E=h

إذن سيكون النص بالكامل هكذا «hqflskhu ph» هذا و نقوم بإرسال النص مشفر و عندما يصل يتم فك تشفيره بعكس خوارزمية التشفير قيصر، تذكر أنه يجب أن يكون الطرف المستلم للنص المشفر لديه المفتاح الذي تم التشفير به الذي هو في مثالنا ٣، نقوم بعكس الخوارزمية بطرح قيمة المفتاح من رقم الحرف، لنحاول فك تشفير النص السابق «hqflskhu ph» حتى نفهم.

الحرف الأول في النص المشفر هو h رقمه ٧، نقوم بطرح ٣ - هي قيمة المفتاح طبعا - من ٧، $7-3=4$ ، الرقم الناتج هو ٤ نبحث عن الحرف المقابل له نجده e، هكذا إلى أن نقوم بتحويل النص مرة أخرى إلى صورته الأصلية.

PlainText Letters : A B C D E F X Y Z
CipherText Lettes : D E F G H I A B C
NETWORKSET

الصورة التالية توضح عملية التشفير و فك التشفير بالمفتاح رقم ٣:
 كسر شفرة قيصر :

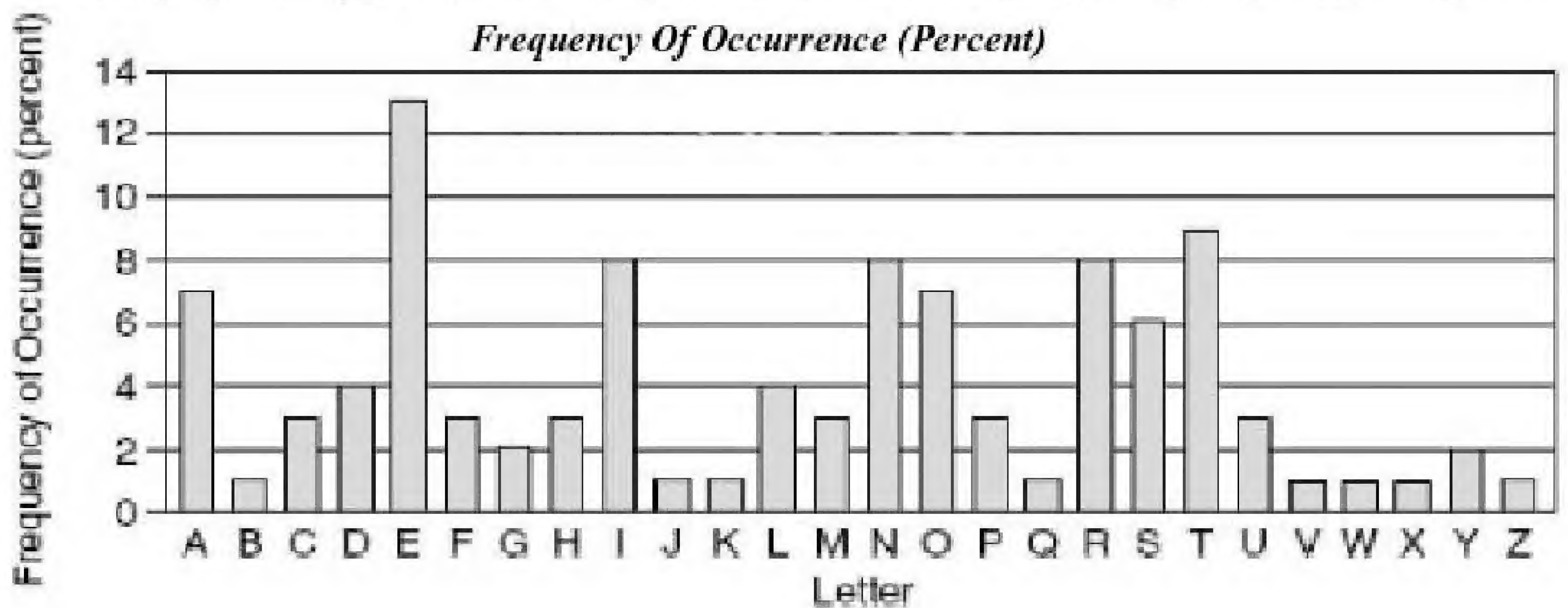
الآن نأتى إلى جزء ممتع و هو كسر شفرة قيصر، و هذه الطريقة تنطبق على جميع خوارزميات النوع Monoalphabetic و لكن سنجربها على المثال السابق، يهمنى جدا أن يفهم القارئ الفرق بين كسر الشفرة و فك تشفيرها، فكسر الشفرة هي مجرد محاولات لفهم شيء من النص المشفر دون معرفة مسبقة لمفتاح التشفير الذي تم إستخدامه، أما فك التشفير فهي العملية السابقة التي قمنا بها لإرجاع النص المشفر إلى أصله. الطريقة التي سنستخدمها في كسر الشفرة تسمى frequency analysis أو التحليل الإحصائي، و هذه الطريقة من

إكتشاف العالم المسلم «أبو يعقوب الكندي» الذي وضع أسس علم كسر الشفرات Cryptanalysis، حيث لاحظ هذا العالم وجود حروف تتكرر أكثر من غيرها في القرآن الكريم.

مثلا أكثر حرف تكررارا في اللغة الإنجليزية هو حرف E، و نلاحظ هذا عند قراءة أى جملة أو نص إنجليزي نجد حرف ال E يتكرر معنا بطريقة ملفتة، ففي مثالنا السابق «Encipher Me» نجد حرف ال E بالفعل هو الأكثر إستعمال و تم تكراره ثلاث مرات، عندما قمنا بتشفير النص السابق كانت النتيجة كالآتي «hqflskhu ph» لو كان أحد منكم قوى الملاحظة سيجد في النص المشفر حرف تم تكراره أكثر من مرة و هو الحرف H، أتكلم عن النص المشفر، و بما أن غالبا في معظم النصوص و الكلمات و الإنجليزية يكون الحرف E هو الأكثر تكرار إذا الحرف h في النص المشفر هو عبارة عن حرف E، بهذا يمكن أن نعرف مفتاح التشفير إذا رجعنا إلى الجدول و قمنا بطرح الرقم المقابل لحرف E من الرقم المقابل لحرف H سيخرج لنا مفتاح التشفير ٣ الذي قمنا باستعماله كتالي ٧ - ٤ = ٣.

هذه هي فكرة التحليل الإحصائي frequency analysis، و بالطبع يختلف الأمر من لغة إلى أخرى و يجب أن يكون عندنا نص كبير نسبيا لكي نتجح هذه الطريقة فمثلا من الممكن أن نقوم بتشفير كلمة أو جملة لا يوجد بها حرف E نهائيا، و عندها يجب ان نجرب ال ٢٥ مفتاح كلهم حتى نصل إلى نص مفهوم حيث أن عدد الاحتمالات لشفرة قيصر هو ٢٥ مفتاح فقط، يمكن لأي جهاز تجريرتهم كلهم في أقل من Milisecond بينما الخوارزميات الحديثة قد تصل عدد المفاتيح فيها إلى أرقام خيالية و ضخمة يحتاج جهاز الكمبيوتر إلى آلاف السنين حتى يقوم بتجربة المفاتيح كلها (هذه ليس مبالغة و سنعرف هذا في الأجزاء المتقدمة من هذه السلسلة). وكما قلت لكم جميع خوارزميات التشفير من النوع Monoalphabetic ضعيفة ضد هجوم frequency analysis. و هذا الجدول يبين نسب تكرار الحروف في اللغة الانجليزية.

هناك طريقة أخرى لكسر الشفرة تسمى Brute-Force Attack لها ترجمة سخيفة هي الهجوم العنيف أو شيء من هذا



القبيل، و تعتمد هذه الطريقة على فكرة تجربة كل المفاتيح المتاحة حتى نصل إلى معنى مفهوم، مثلا في مثالنا السابق نجرب فك التشفير بالمفتاح ١ إذا كان الناتج مفهوما إذا هو المفتاح الصحيح أما إذا كان الناتج كلام غير مفهوم نقوم بتجربة المفتاح التالي، و هكذا حتى نصل إلى المفتاح الصحيح، مشكلة هذه الطريقة هي الوقت ففي شفرة قيصر عدد المفاتيح كلها هو ٢٥ لذلك من السهل أن نقوم بكسر تشفير أى نص مشفر بها عن طريق تجربة ال ٢٥ مفتاح كلهم ، اما لو كان عدد المفاتيح المتاحة في خوارزمية ما هو كدرليون مفتاح مثلا ستحتاج الى وقت كبير لتجربة المفاتيح كلها .

تمرين على كسر شفره قيصر :

قم بكسر تشفير هذه الجملة التي تم إستخدام شفرة قيصر في عملية التشفير، نقوم بترتيب المعطيات أولا:

fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc»«= Cipher Text

??= Plain Text

«Encryption Algorithm = «Caesar Cipher

??= KEY

الخطوة الأولى - نقوم بمعرفة عدد تكرار كل حرف في النص المشفر و سيكون عدد تكرار كل حرف كما في الصورة:

الخطوة الثانية - نلاحظ أن أكثر تكرار في النص المشفر للحرفين n و j حيث تكرر كل منهما ٧ مرات، و بما أن القاعده تقول أن أكثر حرف يتكرر هو ال E، و الحرف الأكثر تكرار في النص المشفر هو J و n إذا يمكن أن يكون الحرف j أو

a:2 , " | b:5 | " , c:3 , d:0 , e:0 , f:3 , g:0 , h:2 , i:0 , " | j:7 | " , k:1 , l:0 , m:1 , n:7 | " , o:0 , p:0 , q:2 , r:1 , s:0 , t:0 , u:3 , v:3 , w:4 , x:3 , y:0 , z:0

NetWorkSet

n يمثل الحرف E، و سنقوم بتجربة كل حرف منهما.

و لحساب المفتاح في الحالة الأولى مع الحرف z نقوم بعملية طرح رقم الحرف e من رقم الحرف z ليكون الناتج هو ٩ - ٤ = ٥، و لحساب المفتاح في الحالة الثانية مع الحرف n نقوم بعملية طرح رقم الحرف e من رقم الحرف n ليكون الناتج هو ١٣ - ٤ = ٩.

إذا المفتاح هو رقم ٥ أو ٩، الآن نجرب الفك بالمفتاح الاول عن طريق طرح رقم المفتاح من رقم كل حرف، فمثلا أول حرف في النص المشفر هو f و رقمه هو ٥، نقوم بطرح ٥ - ٥ = ٠ الناتج رقم صفر وهذا الرقم يقابله حرف a و هكذا إلى أن ننتهي من كل الحروف، و ستكون النتيجة كالآتي:

Cipher Text = «fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc»

Plain Text = «alexw mrere ajevs»

Encryption Algorithm = «Caesar Cipher «

KEY = ٥

توقفت عن عمليه الفك لأن ال plain text الذي ظهر لا معنى له على الإطلاق، إذا المفتاح خطأ و حرف e لا يمثله الحرف z، إذا المفتاح هو ٩، لنجرب ذلك بنفس الطريقة السابقة، أول حرف هو f ورقمه ٥ و المفتاح ٩ و يجب علينا أن نقوم بطرح قيمة المفتاح من قيمة الحرف، و لأن قيمة المفتاح أكبر فسيكون الناتج بالسالب Negative أى ستكون هكذا ٥ - ٩ = -٤، النتيجة هي سالب ٤، في هذه الحالة نقوم بالعد من الخلف أى من الحرف z و نمشي ٤ خانات إلى الوراء _إنظر إلى صورة الحروف و ما يقابلها من أرقام لتستوعب_ و نرى الحرف الذى وقفنا عليه و هو W إذن أول حرف في ال plaintext هو w و الآن أكمل فك باقى الحروف ستجد النتيجة كالآتي :

Cipher Text = «fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc»

« Plain Text = «whats inana mearo sebya nyoth ernam ewoul dsmel lassw eet

Encryption Algorithm = «Caesar Cipher

KEY = ٩

ستجد صعوبة في فهم ال Plain Text إذا لم تكن تتقن اللغة الإنجليزية جيدا لأن حروف الكلمات غير منسقة و بعد تنسيقها ستكون هذه هي الجملة

«whats in a name a rose by any other name would smell as sweet»

ذاكر إنجليزي كويس (-):

طاهر الجمل Egyptian Cryptographer :-

تعموى مصرى و هو أحد العرب القليلين الذين نجحوا في هذا المجال في وقتنا الحالى و له إنجازات كثيرة، عمل في الفترة ما بين عامى ١٩٩٥ إلى ١٩٩٨ كرئيس للعلماء في شركة نتسكيب للإتصالات (Netscape Communications) حيث كان المحرك الرئيسى لبروتوكول SSL، كما شغل منصب موجه الهندسة في شركة (RSA) للأمن قبل أن يؤسس في عام ١٩٩٨ شركة سيكيورفاي (Securify) ويصبح مديرا عاما لها. أيضا هو صاحب حوارزية شهيرة سميت بإسمه ELGamal Algorithm قد نتعرف عليها في أجزاء متقدمة. مسابقه :

فكرت في طريقة أكتشف بها مدى إستيعاب من قرأ هذا المقال و لم أجد طريقة أفضل من عمل مسابقة بسيطة لأكتشف ذلك، سأعطيك نص مشفر بشفرة قيصر بمفتاح مختلف عن الأمثلة السابقة طبعاً، و يحاول كل منكم كسر هذه الشفرة، بعد كسر الشفرة سيظهر لك E-mail ترسل إليه رسالة بأنك إستطعت حل الشفرة (-): .

بصراحة هدفى من هذه الطريقة هو معرفة مدى الإستفادة من هذا النوع من المقالات فإن كان هناك من يهتم بها و يجدها مفيدة سيقوم بفك الشفرة و بهذا أعرف إن هناك من تهمة هذا النوع من المقالات، و سأكمل هذه السلسلة، أما لو لم أجد من يهتم ربما أتوقف عن مواضيع التشفير هذه. فكرت في جائزة و لكن في الوقت الحالى لم أجد شيء أقدمه لمن سينجح في حل هذه الشفرة البسيطة إلا أن أذكر إسمه في العدد القادم، و لكن قد تكون هناك جوائز فيما بعد.

تعليمات المسابقة :

١- قم بفك تشفير هذا النص و تضيف إلى ما سيظهر ymail.com@ أى أن البريد على موقع ياهو.

- ٢- بعد أن تعرف البريد الإلكتروني تقوم بإرسال رسالة إلى هذا البريد بالمواصفات الآتية:
- ال Subject أو عنوان الرسالة تضع في هذه الخانة كلمة NetworkSet.
- ال Message body أو نص الرسالة ستعرفه بعد أن تقوم بكسر تشفير الجزء المكتوب في الصورة التالية بجانب Message Body.

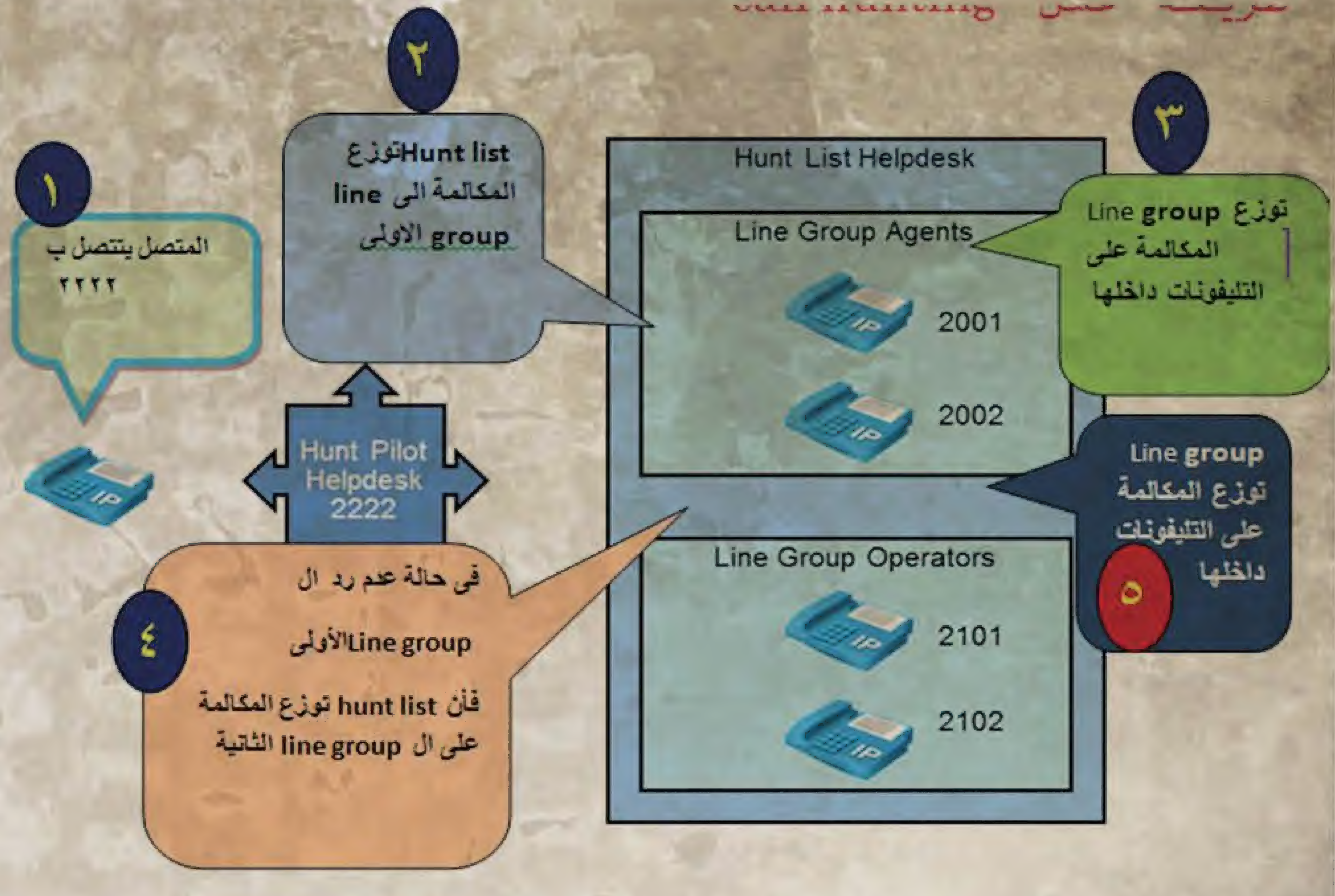
The Encrypted E-mail : yktjskvrkgyk@gmail.com

Message Subject : NetworkSet

Message Body : xfmme pofzp vcsfb luifd pefqm fbtfu zqfzp vsobn fbguf suibu ufyuu ifotf oe

و إلى لقاء آخر في العدد القادم و جزء جديد سنتعرف فيه على خوارزميات أخرى من نوع Cipher Monoalphabetic.

طريقة عمل call hunting



طبعا الخطوات مش محتاجة شرح

بداية من ٤,١ CUCM فإن المكالمات يمكن إعادة توجيهها إلى جهة الوصول الأخيرة عند فشل عملية ال hunting لأي سبب من الأسباب مثل:

إستنفاد جميع خيارات ال hunting ولم يتم أيضا الرد على المكالمة.

٢- نفاذ الوقت المخصص لعملية ال hunting ولم يتم الرد أيضا على المكالمة، وإعادة توجيه المكالمة يتم برمجته في جزء hunting forward setting كما سنرى بالصور لاحقا

ولإعادة توجيه المكالمة لكي لا نفقدها هناك خياران:

يتم وضع رقم وصول شامل لكل المكالمات في hunt pilot .

Personal preference يبرمج في dn للرقم الأصلي المطلوب عند فشل ال hunting لهذا الرقم، ويتم برمجة personal preference بإستخدام إعدادات cfnc على خط التليفون.

طبعا أكيد نسيتموا يعني إيه cfnc، هاقولها وأخذ فيكم ثواب

Cfnc يعني call forward no coverage

ملحوظة :

يمكنك عمل خيار personal preference بواسطة برمجة تليفون المستخدم لكي تجعل خانة fna (forward no answer) تعيد توجيه المكالمة إلى hunt pilot لكي يبحث عن شخص آخر يستطيع الرد على تلك المكالمة، وإذا فشل ال call hunting لأي سبب من الأسباب إما بإستنفاد خيارات ال hunting ، كلها أو لنفاذ الوقت فإن المكالمة تستطيع أن ترسل إلى جهة الوصول الشخصية المحددة للشخص صاحب المكالمة.

مثال

لو تم وضع خانة forward no coverage على البريد الصوتي، فإن المكالمات سوف ترسل إلى صندوق البريد الصوتي للمستخدم صاحب المكالمات في حالة فشل ال hunting .

بعض الإعتبارات التي تطبق على المكالمات التي تعامل ب hunt pilot :

١- Call pickup و group call pickup غير مدعومين على المكالمات الموزعة بطريقة hunt pilot والعضو الموجود في line group لا يستطيع أن يلتقط pickup مكالمات ممررة بواسطة hunt pilot إلى عضو آخر في نفس ال line group وحتى لو كانوا في نفس call-pickup group .

٢- Hunt pilot يستطيع أن يوزع المكالمات إلى أي من أعضاء ال line group بغض النظر عن partition الموجود به العضو و class of service لا تطبق على call coverage .

سؤال : ماهي hunt list ؟
الإجابة:

هي قائمة لها الأولوية من line group تستخدم في call coverage و لها الخصائص التالية:
يمكن أن تشير أكثر من hunt pilot إلى نفس ال hunt list .

يمكن أن تحتوي أكثر من hunt list على نفس ال line group .

Hunt list هي قائمة معطى لها الأولوية من ال line group وهذه ال line groups يتم عمل hunt لها على حسب برمجتها داخل

ال hunt list .

سؤال : ماذا تعرف

عن line group ؟
الإجابة: line group تتحكم في طريقة توزيع المكالمات بين التليفونات وهي لها الخصائص التالية:

Line group تشير إلى تحويلات محددة والتي تكون تحويلات تليفون أو بريد صوتي.

نفس التحويلة يمكن أن توجد في أكثر من line group مختلفة.

Line group تبرمج بطريقة عامة (global distribution algorithm) لإختيار العضو التالي في ال

line group الذي سيحدث له hunting .

تبرمج ال line group بخاصية ال hunt التي تصف كيف سيستمر ال hunting بعد تجربة أول عضو في ال line group . خاصية ال hunt تبرمج لكل حدث فشل في ال hunt على حده مثل: عدم الإجابة، أو إنشغال الخط، أو عدم الإتاحة (no answer, busy, not available).

الوقت سيرن تليفون العضو في line group قبل أن تستمر عملية ال hunting إلى عضو آخر طبقا لإعدادات ال no answer hunt option .

سؤال : ماهي line group members ؟

الإجابة : هي end points ويمكن أن تكون أي شيء من الأنواع التالية

أي جهاز scc مثل التليفونات أو ال ٢٤٨vg ، أو ١٨٨ata .

أجهزة sip .

البريد الصوتي.

أجهزة ٣٢٣.h .

تحويلات fxs المرتبطة ب mgcp gateway .

ملحوظة : منافذ computer telephony integration

ونقاط ال cti route لا يمكن إضافتها إلى line group

ولا يمكن أن تصبح عضوا فيه، ولذلك لا يمكن توزيع

المكالمات خلال تطبيقات cti مثل cisco customer

response solution و cisco unified ip

(interactive voice response (ivr

Call-hunting options and distribution algorithms

هناك العديد من الخيارات المتاحة في ال hunt مثل:

Line Group Configuration

Line Group Information

Line Group Name*	LG1
RNA Reversion Timeout*	10
Distribution Algorithm*	Longest Idle Time

Hunt Options

No Answer*	Try next member; then, try next group in Hunt List
Busy**	Try next member; then, try next group in Hunt List
Not Available**	Try next member, but do not go to next group Skip remaining members, and go directly to next group Stop hunting

Try Next Member, Then, Try Next Group in (Hunt List (Default

ومعناه إذا لم يرد العضو الأول جرب العضو التالي وهكذا جرب كل الأعضاء في نفس ال line group ، فإن لم يرد

أحد في نفس الـ line group ، جرب line group أخرى، فإن لم يرد أحد بداخل الـ line group الثانية حتى تنتهي كل الـ line groups فأوقف عملية الـ hunt .

Try Next Member, but Do Not Go to Next Group

جرب العضو التالي في نفس الـ line group فإن نفذت كل الأعضاء لا تذهب إلى line group أخرى وأوقف عملية الـ hunt.

Skip Remaining Members, and Go Directly to Next Group

لا تحاول مع الأعضاء الآخرين، ولكن عند عدم رد التليفون المطلوب، اذهب مباشرة إلى line group الثانية، وإذا لم يكن هناك line group أخرى فأوقف عملية الـ hunting .

Stop hunting

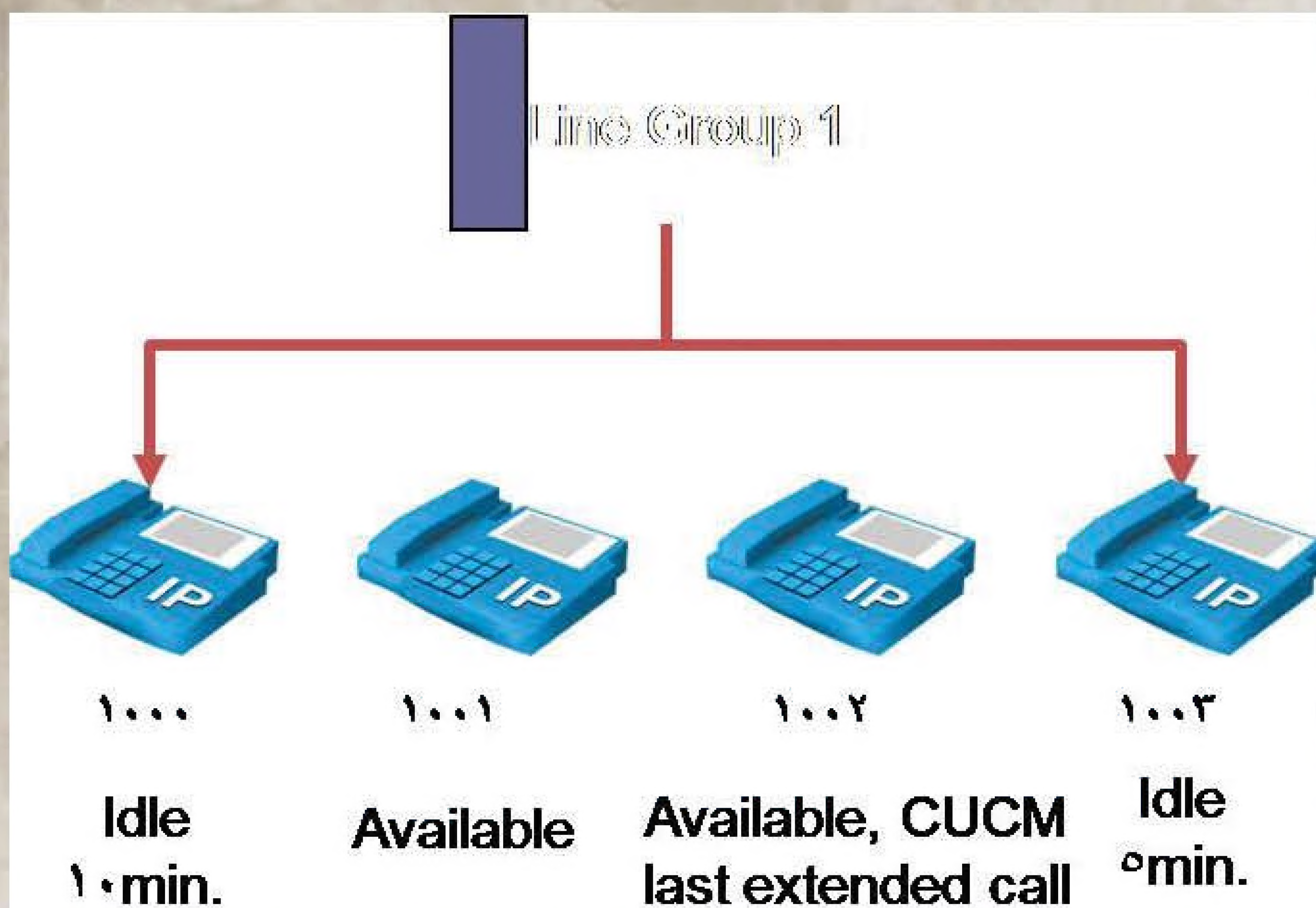
لا تذهب إلى العضو التالي أو إلى الـ line group التالية وأوقف الـ hunting.

Line group distribution algorithm

توضح أي من أعضاء المجموعة سيتم استخدامه أثناء عملية الـ hunting ، وهي على النحو التالي:

Top down

في هذه الطريقة فإن cucm يوزع المكالمات إلى الأعضاء المتاحين أو الـ idle، ويبدأ من العضو الأول متاح، أو الـ idle من القمة إلى العضو الأخير متاح أو الـ idle في قاع الـ line group .



في هذا الشكل ستكون المكالمات لرقم ١٠٠٠، إذا لم يستطع تلقي المكالمات سيرن التليفون رقم ١٠٠١، وهكذا ١٠٠٢، ثم ١٠٠٣، وهكذا سيكون الترتيب من أعلى إلى أسفل، بغض النظر عن الوقت الذي كان فيه التليفون idle . ففي هذه الحالة إذا كان التليفون رقم ١٠٠٠ ليس مشغولاً بمكالمة أخرى أو غير متاح فإنه دائماً هو الذي سيستقبل المكالمات، وفي هذه الحالة سيكون هناك جهد كبير على التليفون ١٠٠٠ .

Circular

في هذه الحالة هو مثل الحالة السابقة ولكن الفرق أنه لن يبدأ من التحويلة الأولى رقم

١٠٠٠، بل كما نرى كان آخر تليفون يستقبل مكالمة لدينا هو التليفون رقم ١٠٠٢، فهنا توجد قاعدة هي $n+1$ حيث n هي آخر تليفون تلقى مكالمة، فيستقبل التليفون الذي يليه في القائمة المكالمات التالية. هذه الطريقة أفضل من الطريقة السابقة لأنها توزع المكالمات على التليفونات، ولا تتسبب بحمل كبير على أحد التليفونات دون الآخر.

Longest idle time

هذه الحالة مختصة بالتليفونات التي في حالة الـ idle فقط، والتليفونات التي ستكون مشغولة أو متاحة لن تستقبل المكالمات وكما نرى المقارنة ستكون بين الرقمين ١٠٠٠ و ١٠٠٣ وطبعاً رقم ١٠٠٠ idle منذ عشر دقائق وسيكون هو الذي سيستقبل المكالمة.

Broadcast

كل التليفونات سترن في وقت واحد المتاحة والـ idle .

سؤال : في أي صفحة من صفحات الـ cucm يتم برمجة الـ distribution algorithm ؟

الإجابة : في الـ line group في cucm administration .

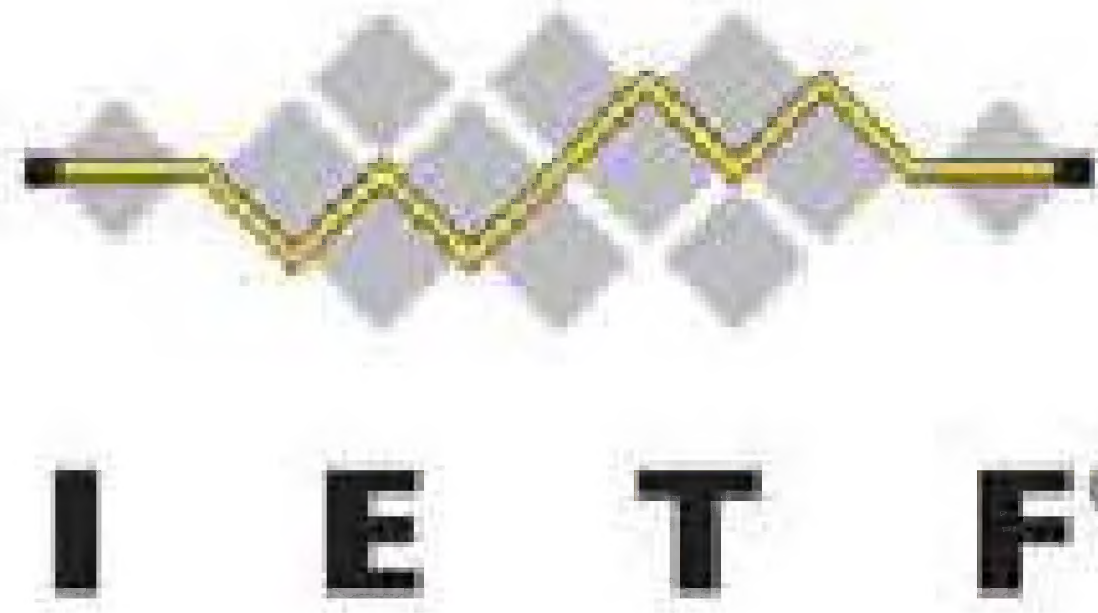
أحمد الشحات

حكومات الانترنت

أيمن النعيمي



قد تكون كلمة حكومة في هذه الأيام شيئاً لاتسر له النفس كثيرا عند سماعها لكن الحكومة التي سوف نتكلم عنها اليوم لاتقتل ولاتضرب بل تؤدي عملها بشكل متقن بعيدا عن الأساليب الملتوية وتقوم بإدارة أكبر عالم موجود على الأرض وهو عالم الأنترنت وهي تدوينتي لهذا اليوم.



ICANN

Internet Corporation for Assigned Names and Numbers (ICANN) وهي اختصار لـ Internet Corporation for Assigned Names and Numbers تأسست هذه المنظمة في كاليفورنيا وتحديدًا في أيلول عام 1998 وهي منظمة غير ربحية وظيفتها الرئيسية هي إدارة وتوزيع الأسماء الحقيقية أو الـ Global IP وهذا يشمل الأصدار الرابع والسادس من الأبي بالاضافة إلى إدارة الـ DNS Root zone أو (TLDs) والذي يعتبر أعلى مكان في التسلسل الهرمي لأي عنوان موجود على الشبكة وأقصد بها طبعاً .net, .com, .org والخ.... يدير هذه المنظمة البروفسور Rod Beckstrom.



ICANN

IANA

وتعني Internet Assigned Numbers Authority وهي وكالة لاتختلف عن الأيكان بشيء وهو سؤال بحثت عنه كثيرا في صفحات الأنترنت وهو الفرق بين الأثنان وتوصلت إلى أن الأيكان هي منظمة قديمة بدأت عملها في نهاية الثمانينات وكانت هي المسؤولة عن كل ما يخص الأنترنت ولكن بعد قدوم الأيكان وحتى لا يختفي هذا الصرح تم عمل ألتفاف على هذه الوكالة بحيث تقوم الأيكان بالأشراف عليها من خلال عقد مبرم بينهم وبذلك تصبح الأيكان هي نفسها الأيكان من ناحية الوظيفة ومن بعض الوظائف التي لم أذكرها توزيع الـ Autonomies System الخاص ببروتوكول الـ BGP وأرقام البروتوكولات والـ DNS ويتبع للأيكان عدة وكالات أخرى تختص كل واحدة منها بقسم معين من العالم وهي على الشكل الآتي :

- ARIN (American Registry for Internet Numbers): North America
- APNIC (Asia-Pacific Network Information Centre): Asia and the Pacific
- RIPE NCC (RIPE Network Coordination Centre): Europe, Central Asia, and the Middle East
- LACNIC (Latin American and Caribbean Internet Address Registry): Latin America and the Caribbean
- AfriNIC (African Network Information Centre): Africa

مختصر هذا الكلام الأيانا تدار من خلال الأيكان لكن هناك وظائف محددة لكل واحدة منها لكن لو سمعنا أن الأيانا هي من يدير ويتحكم بتوزيع الأيبيات فهذا صحيح ولو سمعنا نفس الجملة عن الأيكان فهذا ايضا صحيح.



IETF

وتعني Internet Engineering Task Force وهي منظمة أو هيئة عالمية تتألف من مجموعة كبيرة من المهندسين والذي يتبلور عملهم في تطوير الانترنت وحل مشاكله وتطوير البروتوكولات التي يقوم الانترنت عليها وتقديمها إلى الأيانا على شكل دراسات ووثائق تهدف إلى تطوير بنية الأنترنت ورفع مستواها بحيث يتواءم مع التطور الكبير في عالم التقنية.



I E T F[®]



Echo Technology

Integratoin Technical Solution

Network - Web Design

Training & Development

Programing - Design & Printing

Electronic System - Control System

**Whole Technical
One Supplire**

Study and implementation of engineering projects

**Syria - DeirEzzor - Telefax: 051 218452 - Mob: 0967 96265 - 0955 478942
Website: WWW.EchoTechno.com - E-mail: Info@EchoTechno.com (Soon)**